

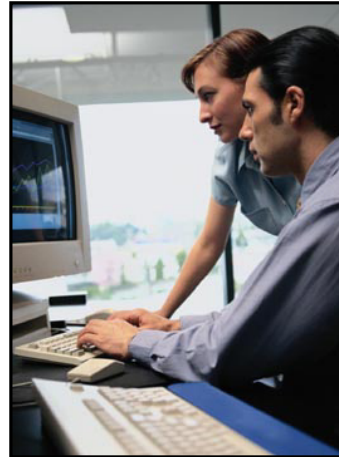
Cisco Network Analysis Modules (NAM) Tutorial

- Cisco Catalyst 6500 Series and Cisco 7600 Series, NAM-1 / NAM-2
- Cisco Branch Routers Series, NM-NAM
- Cisco NAM Traffic Analyzer Software v3.5



About This Tutorial

- **Introduce network performance monitoring concepts and the NAM**
- **Highlight the various features within the NAM modules**
- **View various scenarios explaining how to deploy the NAM and use its features**
- **Provide guidelines for system administrators**
- **Provide links to documentation on the NAM**



About This Tutorial

Welcome to the Cisco Network Analysis Modules (NAM) tutorial! This self-paced training tutorial focuses on Cisco Catalyst 6500 Series and Cisco 7600 Series NAMs (NAM-1, NAM-2), the Cisco Branch Routers Series NAM (NM-NAM), and the embedded NAM Traffic Analyzer software v3.5.

There are two different models of second generation NAMs to support the Cisco Catalyst 6500 and Cisco 7600 series of switches - (WS-SVC-NAM-1/ WS-SVC-NAM-2) that are compliant with the Cisco Catalyst 6500 crossbar fabric architecture. (The first generation NAM part number WS-X6380-NAM is not covered in this tutorial.)

The NM-NAM is a module for the Cisco Branch Routers Series: 2600XM, 2800, 3660, 3700, and 3800 series access routers.

The NAM Traffic Analyzer Software is an embedded, Web-enabled management station that monitors, analyzes, and troubleshoots traffic that traverses the various data sources hosting the NAM-1/2 and NM-NAM hardware. The traffic data collected is based on Remote Monitoring (RMON), RMON2, mini-RMON, Switch Monitoring (SMON) for the Cat6500 NAM, High-Capacity Monitoring (HCRMON), DiffServ Monitoring (DSMON), and Application Response Time (ART) standards.

The NAM provides a wealth of data that can be used for many purposes. This tutorial focuses on how to use the embedded software for configuring the Cat6500 NAM and NM-NAM hardware and software to collect and present data in the format you need.

The tutorial is structured as a series of self-paced modules, or chapters, and concludes with self-administered questions. Also included, in Chapter 5, is a helpful reference section containing links to technical documents on component products, concepts, and terminology. The tutorial material is presented through text, illustrations, hypertext links, and common usage scenarios.

Note(s):

- *Cisco Catalyst® 6500 and Cisco 7600 Series Network Analysis Modules will be referred to, in this tutorial, as the Cat6500 NAM(s), NAM-1, NAM-2 or NAM-1/2.*
- *Cisco Branch Routers Series NAM will be referred to, in this tutorial, as the NM-NAM.*
- *The term NAM refers to all modules, NAM-1, NAM-2, and the NM-NAM.*

How the Tutorial Is Organized

Chapter 1 Introduction to Network Performance Monitoring	Introduce network monitoring concepts and the various Cisco Network Analysis Modules
Chapter 2 Product Features	Learn about the key features for the NAM-1/2, NM-NAM, and the integrated Traffic Analyzer software
Chapter 3 Scenarios	Using several examples, learn how to deploy the NAMs and use the Traffic Analyzer software for viewing the data
Chapter 4 System Administration Guidelines	Review important system requirements, installation guidelines, and system administrative functions
Chapter 5 Helpful Links to Reference Material	A comprehensive set of links to information on the Cisco Network Analysis Modules

How This Tutorial Is Organized

The tutorial is divided into five chapters:

Chapter 1: Introduction to Network Performance Monitoring

This chapter first introduces the user to key concepts in network monitoring. Then the user is introduced to the various NAMs and the embedded Traffic Analyzer software for monitoring network performance.

Chapter 2: Product Features

This chapter discusses the key features of the NAMs (NAM-1, NAM-2, and the NM-NAM) through both discussions of the major functional components and screen shots of specific tasks in the Traffic Analyzer software embedded in the NAMs.

Chapter 3: Scenarios

This chapter walks you through step-by-step examples to provide hands-on experience using features of the various NAM modules (NAM-1/2 and NM-NAM) and the embedded Traffic Analyzer software. The case studies begin with steps on how to get started, followed by various scenarios on performance monitoring, troubleshooting the network, analyzing DiffServ, application response time monitoring, monitoring VoIP, and generating traffic and performance reports.

Chapter 4: System Administration Guidelines

This chapter provides important information about installation guidelines, hosting requirements, client web browser specifications, initial configuration of the hardware, and periodic maintenance topics.

Chapter 5: References

This chapter contains a list of additional product information, such as links to related white papers and documentation.

Tutorial Contents

Chapter 1 – Introduction to Network Performance Monitoring

- Network Performance Monitoring
 - **The Need To Manage Network Traffic**
 - **Business Metrics, Data to Collect**
 - **The Key to Performance Monitoring**
 - **Understanding MIBs and RMON**
- Introducing Cisco's Network Analysis Modules and Software
 - **Deploying NAMs**
 - **Cisco Catalyst 6500 Series and Cisco 7600 Series NAM-1/2**
 - **Cisco Branch Routers Series NM-NAM**
 - **Cisco NAM Traffic Analyzer Software**
- Cisco Complementary Solutions
- Summary – Benefits Achieved

Chapter 2 – Product Features

- Network Monitoring Using NAMs
 - **Deploying NAMs**
 - **Understanding Data Sources**
- NAM Hardware Overview
 - **Catalyst 6500 and 7600 Series NAM-1/2**
 - Features
 - Specifications, Comparison of NAM-1, NAM2
 - Architecture
 - Data Sources
 - **Cisco Branch Routers Series NM-NAM**
 - Features
 - Specifications
 - Architecture
 - Data Sources
- Traffic Analyzer Software
 - **Planning**
 - NAM Placement
 - Performance Considerations
 - Security

Chapter 2 – Product Features, continue ...

- Traffic Analyzer Software
 - Planning**
 - Getting Started**
 - NAM Hardware Installation
 - NAM User Interface
 - NAM Network Configuration
 - Securing Access to the NAM
 - Viewing Access Logs
 - Setting NAM System Time
 - Configuring**
 - Basic NAM-1, NAM-2 Configuration
 - Overview of Steps
 - Configuring Data Sources
 - Enabling Core Monitoring
 - Basic NM-NAM Configuration
 - Overview of Steps
 - Configuring Data Sources
 - Enabling Core Monitoring
 - Types of Statistics Collected
 - Enabling Traffic Monitoring
 - Configuring Alarms
 - Setting Preferences
 - Viewing Reports**
 - Viewing Real-Time Reports
 - Types
 - Layout
 - Selecting Data Source
 - Common Error Messages
 - Standard Reports
 - Real-Time Trending
 - Drill-Down
 - Health
 - Creating and Viewing Historical Reports
 - Viewing Alarm Logs
 - Data Capture**
 - Buffers
 - Capture Settings
 - Quick Capture
 - Decoding Captures
 - Saving to Hard Disk

Chapter 3 – Scenarios

- Performance/Troubleshooting (NAM-1/2)
- Performance/Troubleshooting (NM-NAM)
- QoS Monitoring (Using DiffServ and ART)
- VoIP Monitoring
- Trend Analysis

Chapter 4 – System Administration Topics

- Requirements
 - Hosting Hardware and Software
 - Client (Access to the NAM Using a Web browser)
- Administration
 - NAM-1, NAM-2
 - Install and Verification
 - Initial Configuration
 - NM-NAM
 - Install and Verification
 - Initial Configuration
- Maintenance
 - Resetting the NAM
 - Image Upgrade
 - NAM-1, NAM-2
 - NM-NAM
 - Patch Installation
 - Shutdown
- Troubleshooting Tips

Chapter 5 – References (Links to More Documentation on Related Topics)



Introduction

Chapter 1



Chapter 1 Outline

- **Network Performance Monitoring**
 - The Need To Manage Network Traffic
 - Business Metrics, Data to Collect
 - The Key to Performance Monitoring
 - Understanding MIBs and RMON
- **Network Analysis Modules**
 - Deployment
 - Cisco Catalyst 6500 Series and Cisco 7600 Series NAM-1/2
 - Cisco Branch Routers Series NM-NAM
- **Traffic Analyzer Software**
- **Cisco Complementary Solutions**
- **Summary – Benefits Achieved**

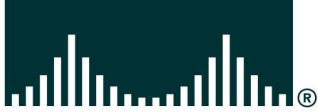


Chapter 1 Outline

Before introducing the NAMs and its embedded Traffic Analyzer software, the first step is to acknowledge the importance of performing network performance monitoring in today's environment. As will be discussed, there is a real need for monitoring the network proactively; however, the effort to collect and analyze the necessary data is often time-consuming, repetitive, and often difficult to interpret.

This will set the stage to introduce the need for a tool to collect and analyze the traffic traversing the network. The NAM and the embedded software is presented as Cisco's solution to performing network performance monitoring to achieve all the benefits while minimizing the challenges. Chapter 2 will focus on all the features of both the Cat6500 NAM and the NM-NAM, followed by usage scenarios in Chapter 3. Finally, Chapter 4 will present further administrative information for installing, accessing, configuring for initial use, and maintaining the NAM.

CISCO SYSTEMS



Network Performance Monitoring

- The Need
- Business Metrics, Data to Collect
- The Keys to Performance Monitoring
- Understanding MIBs and RMON

Network Analysis Modules

Traffic Analysis Software

Cisco Complementary Solutions



Network Performance Monitoring

The Importance of Monitoring Network Traffic

No longer is it enough ...

- To only react to problems...you must also be proactive
- To alarm or alert to an outage or service degradation....you must receive information before it occurs
- To insure traffic flow from one point to another.....must insure optimum performance of that traffic...
- To understand that network , traffic or applications are slow...you must understand “why”
- Make assumptions about projected capacity decisions..you need fact to justify expenditures / return on investment (ROI)

Intelligent Information Network

Cisco's 3-5 year vision for the evolution of networking from connectivity to intelligent systems



The Need to Manage the Network Traffic

Network administrators and corporate executives understand that monitoring the network is important and vital to business operations. It is not simply enough to know if a device is down or the network is slow. Network administrators need to be more proactive by monitoring the devices and the network and watching for trends or deviations from an established baseline.

And when there is a problem, resolving the problem quickly means having the right information to make decisions. This information can only be obtained by monitoring the application traffic, to understand who is generating the traffic and where the traffic is going.

Additionally, if more bandwidth is warranted, the recommendations will need to be justified. Network monitoring can provide this cost justification. Thus, visibility into the performance of networks and the systems and applications that run on them is essential. By gaining visibility into the network, network administrators can more proactively resolve problems before they arise, plan for changes in resource usage, and manage valuable network resources.

Cisco makes this job easier than ever by providing visibility into the network. Cisco is making the network easier to manage by building intelligence into the devices!

Network Performance Monitoring

Business Metrics for Evaluating Performance

- **Response Time:** The elapsed time between the end of a query on one end of a conversation pair and the beginning of a response from the other end of a pair. Latency, a function of response time, is any characteristic of a network or system that increases the response time.
- **Reliability:** A measurement of the consistency of any network, system or application in performing according to its specifications.
- **Device or Interface Utilizations:** The amount of data moved successfully from one place to another in a given a specified amount of bandwidth.
- **Network Utilization Patterns:** Trending how the network is being used, by protocols, users, and how the patterns are changing.



Business Metric for Evaluating Performance

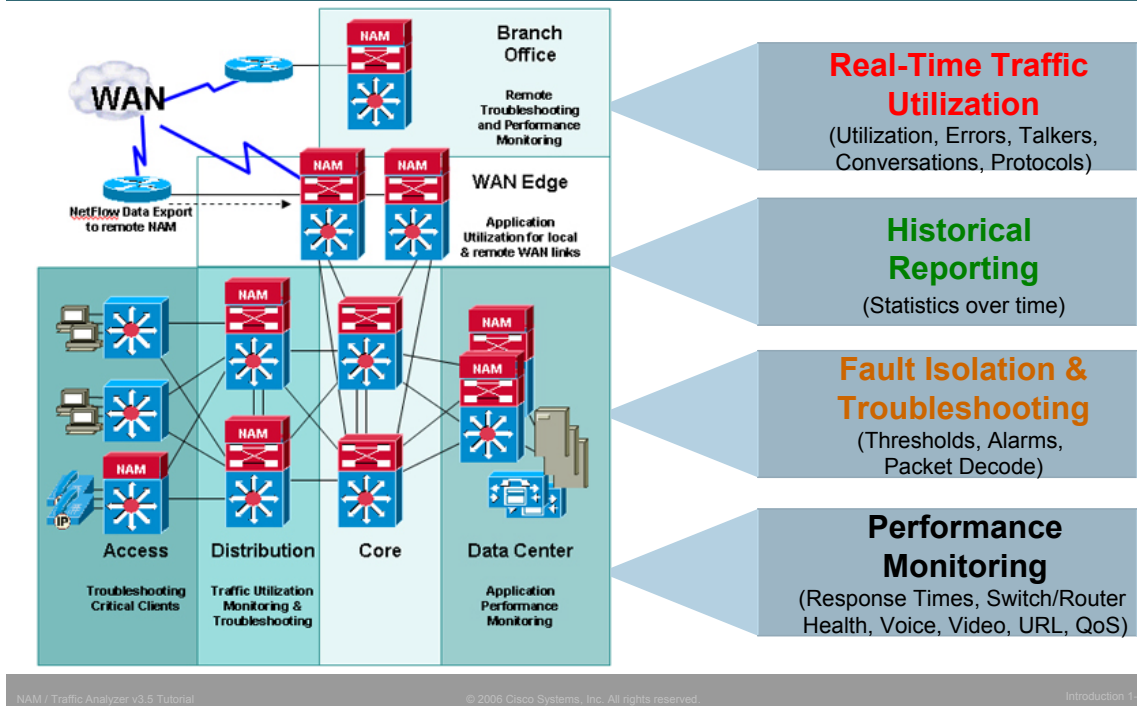
Measuring the health of the network is done typically using business performance metrics. These metrics include, but are not limited to:

- **Response Time:** The elapsed time between the end of a query on one end of a conversation pair and the beginning of a response from the other end of a pair. Latency is any characteristic of a network or system that increases the response time.
- **Reliability:** A measurement of the consistency of any network, system or application in performing according to its specifications.
- **Utilization:** The percentage of total bandwidth used for transporting data. Utilization is often monitored on an ongoing basis for evaluating the usage of the network over time for capacity planning purposes.

These metrics can be used to evaluate how well network, system, and application resources are performing, and how these resources affect the delivery of network services both for present analysis and future planning. Now let us look at some of the sources of data that is used to perform real time monitoring and historical reporting functions.

Network Performance Monitoring

Different Monitoring Points for Application Usage



What Data to Collect

The network management plan may identify the performance requirements based on the previously mentioned performance metrics. But how can these metrics be calculated? What data should be collected from the network to determine if the network is meeting the performance requirements?

The figure above illustrates various reasons for collecting performance statistics at different points in the network. Directly at the access port, statistics on port utilization, errors, and packet size distribution can be obtained either from the Cisco MIB or the RMON MIB, both embedded on Cisco switches. These statistics are useful for trending and baselining the port usage and it would not be necessary to monitor all user ports. But when more visibility into the traffic upper layers and understanding who's talking to who in the network is needed, simply looking at interface statistics is not enough.

Network Performance Monitoring

What Data to Collect

- **Port level statistics—utilization, collisions, fragments**
 - Basic physical stats good for usage trending and baselining
 - Useful anywhere in the network
 - Not necessary for all user ports
- **Detailed physical, network, and application layer data**
 - Collect layers 2-7 statistics for understanding traffic breakdown
 - Valuable for WAN aggregation links
 - Valuable for LAN aggregation links (building to building, distribution to core, server farm to core)
- **What collection interval?**
 - Shorter intervals for real-time monitoring and troubleshooting (5–30 sec)
 - Longer intervals for historical trending (5 min–15 min)



What Data to Collect, continue ...

Port level or interface statistics is the first alarm when issues arise. These statistics are available most of the time by simply querying the interface MIB. It may only be necessary to monitor these statistics at critical points in the network and not at all access points.

Collecting statistics at upper layer protocols (network through application) would require the use of an RMON II probe or analyzer, such as the NAM. RMON II would provide visibility into who is (applications, hosts, conversations) using valuable WAN or LAN resources at the core or distribution layers and at the WAN edge or access layer.

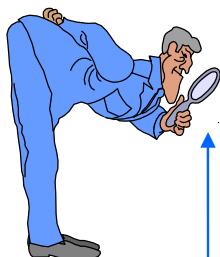
Always an important consideration is how often these statistics should be collected. Rule of thumb: if the data is needed for real-time troubleshooting then the polling frequency should be often; whereas, if the data is needed for long term trending and placed into a database, then the polling frequency should be shorter and average over a longer period of time.

Let's look more in depth at the data collected at the RMON I and RMON II standards.

Network Performance Monitoring

The Key to Performance Monitoring

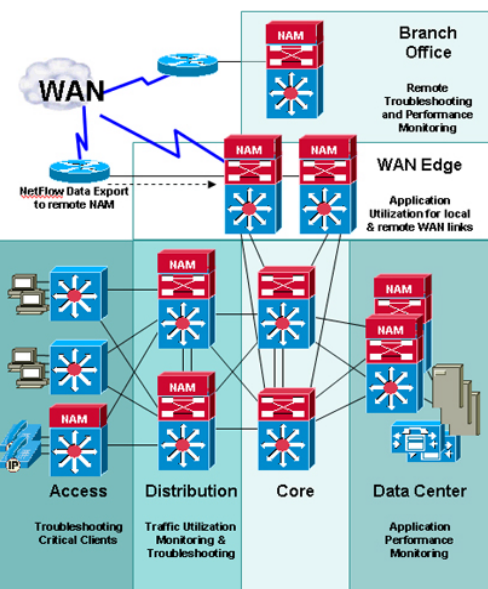
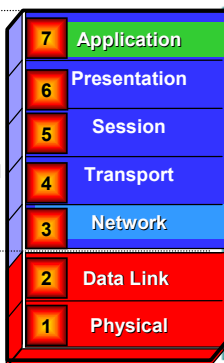
Obtain “visibility” into the network at the upper layer protocols



OSI
Protocol
Layers

RMON-2
Standard

RMON-1
Standard



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction 1-14

Visibility: The Answer to Some of Our Monitoring Needs

What is needed to solve some of the challenges that you face when it comes to monitoring your network? Visibility, the ability to see and analyze the traffic that consumes the resources on your network, will help you solve many of the management problems just mentioned. Visibility means many things in the context of today's complex networks, so to understand what is required and why, let's look at the issues in more detail.

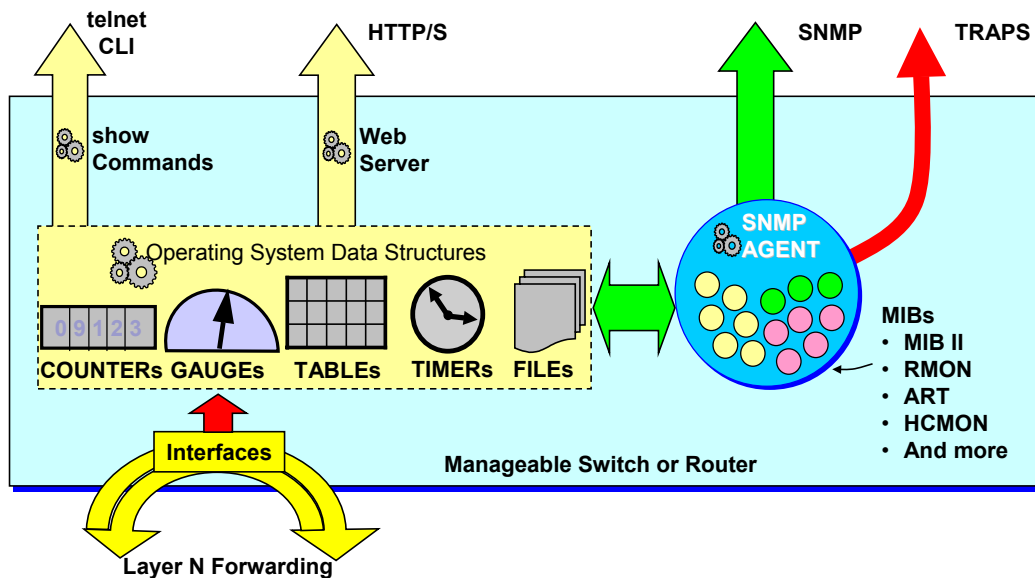
Network traffic consists of discrete units called packets. Everything you want to know about the traffic on your network exists in the protocol headers of a packet. By examining the headers that are created at different protocol layers, you can identify who is talking with whom, what QoS priority has been assigned to a packet, what application created the packet, and so on. Just from the information in the packet headers, you can create very meaningful reports that help you understand how your network is being used. Collecting information from the packet itself is the best way to gain visibility into your network.

But visibility is not just about what you gather, it is also about where you gather it from. For example, most networks today employ some form of layer 2 switching and VLANs at critical points in the network such as aggregation points and server farms where a significant percentage of network traffic converges. Collecting data from a switch itself provides visibility into the packets that traverse your network, the switch fabric, the switch ports that provide access to application servers, and trunk ports where traffic aggregates. Additionally, monitoring traffic at the edge of the network provides visibility into the users and applications at crucial access points or at costly WAN links.

Monitoring directly at the Catalyst switch or branch router provides other benefits as well. It also offers the ability to monitor critical devices, such as servers, closest to their source at the port that connects the devices to the network. This enables you to collect information from a response-time perspective because traffic can be time stamped as it enters and exits ports. Collecting response-time data provides a direct way to measure the end user's experience of your network. That is visibility!

Network Performance Monitoring

Understanding the Basics



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction 1-15

Understanding the Basics

Let's now look inside an intelligent switch or router. Many network-based devices have built-in intelligence to assist in management activities. As traffic traverses the device interfaces, information about the amount and type of traffic seen is stored in various operating system data structures, consisting of counters, gauges, tables, timers, and files. The retrieval and/or modification of this information can be achieved through numerous communication protocols (depending on the device type) including the traditional Command-Line Interface (CLI), telnet, HTTP, Syslog, and TFTP.

In an effort to standardize the mechanism used for device status information necessary for network management tasks, the Management Information Base (MIB) information model was created. The information stored in these data structures is stored in standardized MIBs. The content within the MIBs are well documented and easy to access using the MIB object identifier.

Likewise the Simple Network Management Protocol (SNMP) was chosen as the standardized communication model for retrieving information held by the MIB, as well as alert IT managers to conditions occurring within the managed device using SNMP traps.

Network Performance Monitoring

Understanding MIBs - RMON I MIB (Layers 1 & 2)

- 1 ★ **statistics** » Real Time Physical and Data Link Layer Statistics
- 2 ★ **history** » Statistics Over Time
- 3 ★ **alarm** » Predetermined Thresholds Set on Statistics
- 4 **host** » **Talker Statistics – Data Link Layer**
- 5 **hostTopN** » **Top N Talkers - Data Link Layer**
- 6 **matrix** » **Conversation Statistics– Data Link Layer**
- 7 **filter** » Packet Structure and Content Matching
- 8 **capture** » Packet Capture for later analysis
- 9 ★ **event** » Reaction to Predetermined Conditions (threshold reached)
- 10 **tokenRing** » Token Ring - RMON Extensions



Mini-RMON – Can be enabled on all Cisco Catalyst ports

Understanding MIBs – RMON I MIB

One such MIB is the RMON I (Remote Monitoring) MIB. The RMON MIB is a standard MIB included as a subtree off the MIB2 subtree. RMON, in brief, collects the following:

- *Basic layer statistics* - line utilization, packets, and errors; and protocol utilization and packets
- *Host Statistics* – byte and packet counts to and from a host (by MAC address at the data link layer, network address at the network layer, and network address at the application layer).
- *Conversation statistics* - byte and packet counts from one host to another (by MAC address at the data link layer, network address at the network layer, and network address at the application layer).
- *Packet Capture* – RMON can be used to capture a subset of network traffic for detailed protocol analysis.
- *Thresholds and Alarms* – RMON can set up thresholds to look for various conditions (e.g. link utilization greater than 70% for 60 seconds) and inform a management station with an SNMP trap when the condition occurs.

Since the amount of statistics gathered per interface, most RMON implementations are in stand-alone network devices often called RMON analyzers, such as the NAM. The exception to this is the use of a small subset of RMON implemented on a switch to collect basic data-link layer statistics, a brief history of these statistics, and the ability to set thresholds against the statistics all on a per port basis. This subset of RMON is known as mini-RMON (Statistics, History, Alarms, and Events).

Network Performance Monitoring

Understanding MIBs - RMON II MIB (Layers 3 - 7)

11	protocolDir	» Master List of Protocols seen on data source
12	protocolDist	» Protocol Statistics
13	addressMap	» Host to MAC Address Matching List
14	nlHost	» Talkers Statistics - Network Layer
15	nlMatrix	» Conversations Statistics - Network Layer
16	alHost	» Talkers Statistics - Application Layer
17	alMatrix	» Conversations Statistics - Application Layer
18	usrHistory	» Data Logging - User Specified Variables
19	probeConfig	» Probe Configuration Standards

Understanding MIBs – RMON II MIB

RMON II offers extensions to the RMON I standard by providing statistics beyond the Data Link Layer (layer 2). Statistics are available on the Network Layer through the Application Layer.

Basically, RMON II looks deeper into every packet it analyzes to detail which network layer addresses are consuming the most bandwidth, which network layer addresses are talking to each other, and which applications, identified by port numbers, are consuming bandwidth.

Network Performance Monitoring

Understanding MIBs – Protocol Directory Extensions

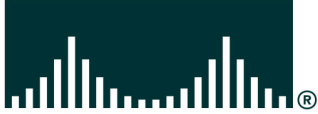
- **Application Response Time (ART)**
- **Voice / Video**
- **Differentiated Services (DSMON)**
- **NBAR-PB MIB** *Branch Router NM-NAM*
- **Switch Monitoring (SMON)** *Catalyst 6500 and 7600 Series NAM*
- **Usage per Virtual link** *Catalyst 6500 and 7600 Series NAM*
 - VLAN
 - VLAN Priority
 - VLAN ACL

Understanding MIBs – Protocol Directory Extensions

The NAM not only implements the full RMON2 specification, but also implements additional monitoring features to support technologies in use today.

- *Application Response Time (ART)* - Stores response-time statistics on client/server requests and responses
- *Voice / Video* – Monitoring voice and video protocols (SCCP, H.323, MGCP, SIP, RTP) for packet loss, jitter, call or video stream details.
- *DSMON (Differentiated Services Monitoring)* – Equivalent to putting an RMON agent on each traffic flow defined by differentiated services code point (DSCP) value. Allows a user to see which DSCP group is putting the most traffic on the link, and which users within the DSCP group are consuming the bandwidth. This data can be analyzed to "tune" DSCP allocations within a network, based on the quality of service (QoS) policies for that network. Network managers can also guard against QoS policy violations by monitoring DSCP usage by applications other than the designated ones.
- *NBAR-PB (Specific to the NM-NAM)* – Network-Based Application Recognition statistics. Statistics on application traffic seen on each interface of the router is collected.
- *SMON (Switch Monitoring – Specific to the Cat6500 NAMs)* – Similar to RMON1 except for a switch as opposed to a shared medium. Provides more visibility into traffic traversing a switch.
- *Per Virtual Link Monitoring (Specific to the Cat6500 NAMs)* Equivalent to putting an RMON agent on the virtual entity itself allowing for more precise visibility into the consumption of a link. Not only which virtual entity is consuming the most bandwidth, but also who within the virtual entity is responsible for consuming bandwidth.

CISCO SYSTEMS



Network Performance Monitoring

Network Analysis Modules

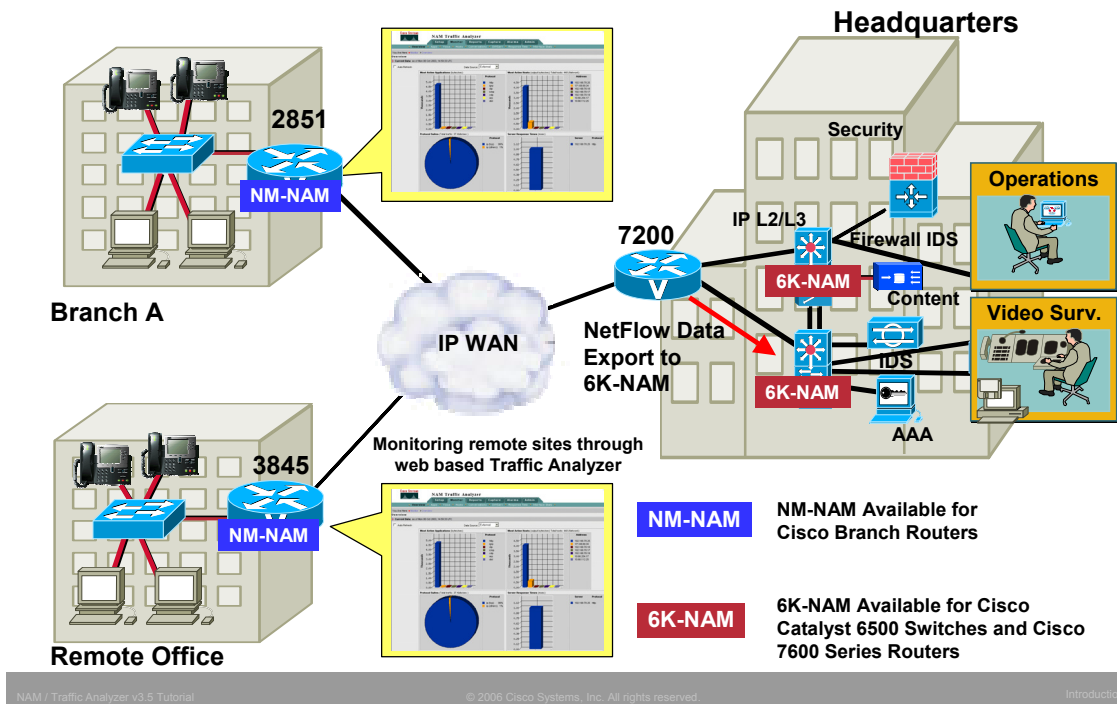
- Deploying NAMs
- Cisco Catalyst 6500 Series and 7600 Series NAM-1/2
- Cisco Branch Routers Series NM-NAM

Traffic Analysis Software

Cisco Complementary Solutions



Network Analysis Modules Deployment



Deployment

Collecting the data you need is made easier and flexible by the functionality of the NAM to be placed where it is needed and gathers data from either local or remote switches and routers.

Cat6500 NAMs

The Catalyst 6500 series switches and the Cisco 7600 series routers can host the NAM-1 or NAM-2. These NAMs can collect and display per port layer 2 statistics in conjunction with the mini-RMON on every interface. More in-depth analysis of LAN ports can be achieved by spanning or copying traffic from ports, VLANs, or Ether Channels to the embedded NAM or by using VLAN Access Lists (VACL) to mirror data to the NAM if no spanning sessions are available.

Analysis of remote switches can be achieved using the Remote SPAN (RSPAN) and Encapsulated SPAN (ERSPAN) features of Catalyst switches. (*Refer to Chapter 2 for details on RSPAN and ERSPAN.*) Detailed analysis of WAN ports can also be achieved by using VACLs on a local device or by forwarding NetFlow data from either the local or a remote device.

The Cat6500 NAMs can monitor traffic running at sub gigabit speeds (NAM-1) and gigabit speeds (NAM-2) and provide enormous value when deployed at the following areas:

- Distribution or core layer trunk ports
- Service points (for example, in data centers, server farms, or Cisco Call Manager clusters in IP telephony) where performance is critical
- Critical access points

NM-NAM

The Cisco Branch Routers Series NAM, NM-NAM, is an integrated traffic-monitoring network module for Cisco 2600XM, 2800, 3660, 3700, and 3800 series access routers that enables network managers to gain application-level visibility into traffic at **remote sites** or at the **WAN edges** to improve network performance, reduce failures, and maximize returns on investments. It expands the NAM solution available for the Cisco Catalyst 6500 series and Cisco 7600 series by allowing remote troubleshooting and traffic analysis without having to send personnel to remote sites or hauling large amounts of data to the central site. The NM-NAMs can collect MIB-II statistics on each interface.

Network Analysis Modules

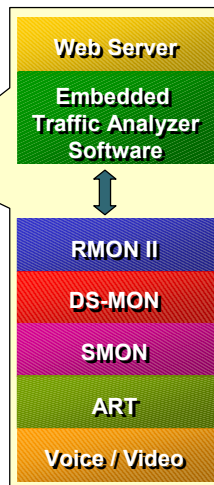
Cisco Catalyst 6500 / Cisco 7600 Series NAM-1/2

Catalyst 6500 and Cisco 7600 Series



**NAM-1, NAM-2
Blade**

**Port (mini-RMON)
statistics are available
on each interface**



HTTP/S



**Capture/Decode
Packets**



Cisco Catalyst 6500 and Cisco 7600 Series, NAM-1/2

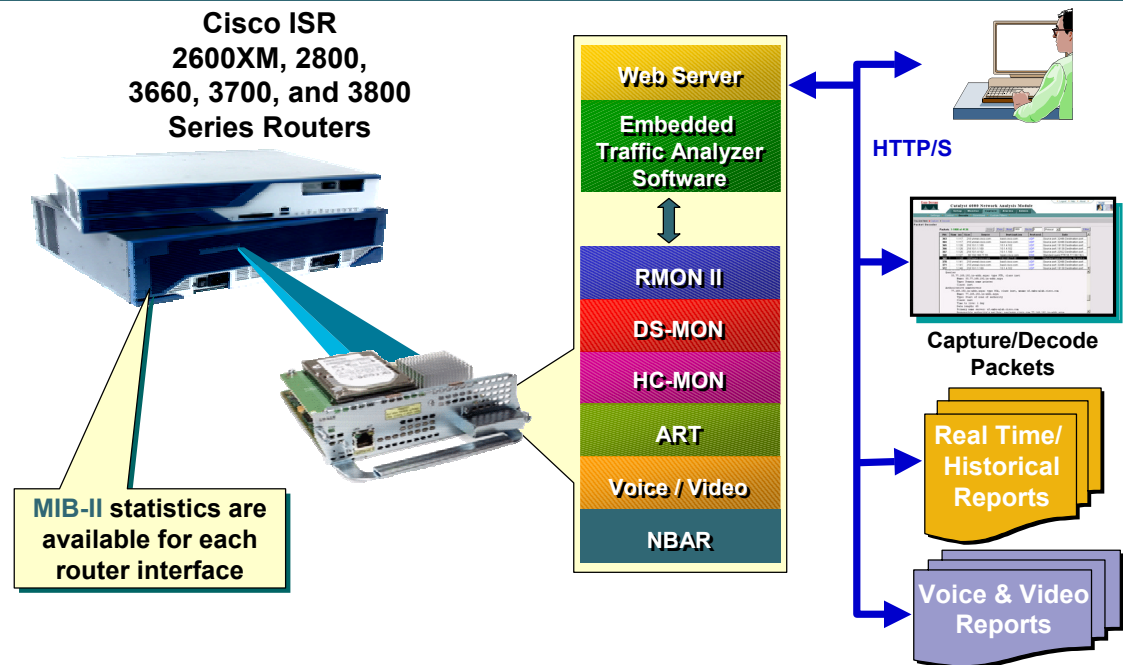
With the NAM, Cisco offers a solution that provides network visibility while also addressing many of the network and performance monitoring issues that have been raised. What is the NAM exactly? The Network Analysis Module (NAM) for Cisco Catalyst 6500 series switches and Cisco 7600 series Internet routers, referred to herein as the Cat6500 NAM, is a network monitoring system that combines a rich set of embedded data collection and analysis capabilities with a web-based management console. And all of this functionality resides in a single module. In addition, the NAM has dedicated resources for all management functions, thus eliminating any load it might impose on the host switch. Now, large volumes of performance data can be gathered about the switch and the traffic traversing it without impacting the switch itself.

What does the NAM look like from the inside? Well, it is basically a fully integrated management system that gathers information at the packet level for any interface, VLAN, or Cisco Ether Channel® tunnel on the switch. It includes embedded Traffic Analyzer software that analyzes and stores the data using both standards-based and proprietary MIBs (Remote Monitoring, DiffServ Monitoring, Switch Monitoring, Application Response Time Monitoring, and VoIP Monitoring). The value of each of these MIBs will be explained throughout the tutorial.

The NAM also hosts an embedded Web server that presents the configuration menus and traffic reports generated by the Traffic Analyzer software to clients using a supported Web browser. These reports can provide visibility into voice or data traffic, VLANs, DiffServ configurations, hosts, conversation pairs, application usage, or application response times. With the NAM, you have the ability not only to collect packets, but to collect them from the switch itself, giving you the flexibility and visibility to see into the smallest details of how your switch and your network is being used and how your users experience the services your network offers.

Network Analysis Modules

Cisco Branch Routers Series NM-NAM



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction 1-22

Cisco Branch Routers Series NM-NAM

Cisco Branch Routers Series NAM, referred to herein as the NM-NAM, internally, is very similar to the Cat6500 NAMs. The NM-NAM is available for Cisco 2600XM, 2800, 3660, 3700, and 3800 series access routers to gain application-level visibility into traffic at remote sites. Just like the Cat6500 NAM, the NM-NAM provides detailed analysis of applications, hosts, conversations, and network-based services such as quality of service (QoS) and voice over IP (VoIP). The NM-NAM also includes the embedded, web-based Traffic Analyzer software, which provides full-scale remote monitoring and troubleshooting accessible through a web browser.

The NM-NAM is *slightly different* from the Cat6500 NAM in the following ways:

- The SPAN or copy network traffic for analysis is a feature of Catalyst switches and not of branch routers. Instead of receiving SPAN, the NM-NAM receives duplicates of packets either directly from the router backplane in a passive or promiscuous mode using a special packet-monitoring feature in Cisco IOS® Software, or through an external Fast Ethernet interface.
- The capability of monitoring VLANs is a layer 2 feature and is not supported in the routers.
- Catalyst 6500 / Cisco 7600 series devices support interface monitoring using mini-RMON. The branch routers can provide similar interface monitoring by the NM-NAM using the MIB-II statistics available on each router interface.

Let's now look at the Traffic Analyzer software embedded in both the Cat6500 NAMs and the NM-NAM.

CISCO SYSTEMS



Network Performance Monitoring

Network Analysis Modules

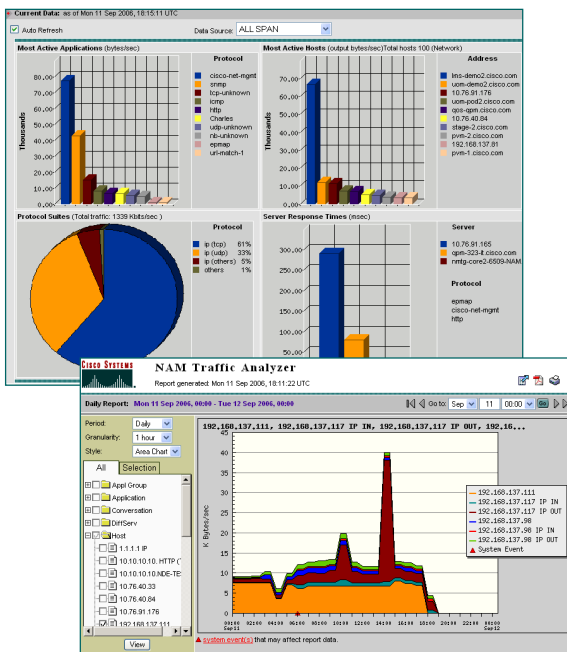
Traffic Analysis Software

Cisco Complementary Solutions



Traffic Analyzer Software Overview

- **Configuration of the NAM**
 - Setup Network Parameters
 - Selection of traffic to monitor
 - Define types of statistics to collect
- **Real-Time and Historical Reports**
 - Switch Port Monitoring (NAM-1/2)
 - Router Interface Monitoring (NM-NAM)
 - Application, Hosts, and Conversation Monitoring
 - Differentiated Services (DiffServ) Monitoring
 - Voice / Video Quality Monitoring
 - Application Response Time Monitoring
 - URL Monitoring
 - Packet Capture and Decode
 - IP / MPLS Monitoring (NAM-1/2)
 - VLAN Monitoring (NAM-1/2)
 - Overall System Health



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction 1-24

Traffic Analyzer Software - Overview

The Traffic Analyzer software is embedded in both the Cat6500 NAMs and the NM-NAM and accessible using HTTP/S from a web browser.

The Traffic Analyzer software not only allows the user to configure the NAMs for monitoring, but also monitoring traffic for various network usage situations and provides many reports on how the network is being used.

Let's look briefly at the different ways the Traffic Analyzer can be used for monitoring network traffic. These features of the Traffic Analyzer software will be discussed in greater detail in Chapter 2 and 3 of this tutorial.

Port Statistics

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Count Types:

Traffic Rates
Error Rates
All

 Port Name:

Showing 1-5 of 5 records

	#	Name	Utilization %	Bytes/s	Packets/s	Broadcast/s	Multicast/s	Errors/s
<input type="radio"/>	1.	Fa4/1 (CONNECTION TO NMTG-HQ-CORE-7200)	0.03	8,271.37	40%	14.48	0.00	0.36
<input checked="" type="radio"/>	2.	Gi3/2	0.00	7,744.57	37%	11.40	0.00	0.18
<input type="radio"/>	3.	Gi1/2	0.00	4,429.50	21%	38.81	1.40	18.22
<input type="radio"/>	4.	Gi1/3 (CONNECTION TO NMTG-DEMO-8500)	0.00	222.68	1%			
<input type="radio"/>	5.	Gi1/1 (CONNECTION TO NMTG-HQ-DIST-6509)	0.00	47.68	<1%			

Rows per page: Units:

View traffic and error statistics for all interfaces by selecting an interface and drill down into the interface to obtain more details

Port-level statistics include:

Utilization, packets, errors, collisions

**Real-Time &
Historical
Reports Available**

Switch Port Monitoring

Naturally, you would expect the NAM to provide port-level monitoring for the host Cisco Catalyst® switch, and of course it does. Switch monitoring and reporting is available for every port on the switch, regardless of the NAM configuration. In other words, switch port monitoring is always available because it is the very foundation of performance monitoring and troubleshooting. In fact, troubleshooting always begins with a review of statistics.

Using port statistics, you can gather important information about the switch performance as well as utilization patterns. Switch port statistics include packet and byte counts as well as port utilization. It also includes error statistics such as cyclic redundancy check (CRC)/alignment errors, oversized and undersized frames, fragments, jabbers, and collisions. It also provides information on broadcast and multicast activity. In addition, you can also configure the NAM to notify you when any of these values exceeds the thresholds you have defined for them.

The NAM gathers these statistics from the mini-RMON agent in the Cisco Catalyst switch. No overhead is added by collecting these statistics, and you can use them even when you configure other data sources for the NAM such as VLANs or Cisco EtherChannel® tunnels and you will still continue to collect port statistics. However, if you want more information than the mini-RMON statistics provide, such as network layer host or conversation pair data or application protocol data, then you can always copy traffic from any combination of ports on the switch to the NAM to provide more insight. (A switch can be configured to copy or mirror port or VLAN traffic and send it to a Switched Port Analyzer [SPAN] port for further analysis; this procedure is called **spanning**.)

Interface Statistics

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data													
Filter: <input type="text"/> <input type="button" value="Filter"/> <input type="button" value="Clear"/>													
Showing 1-4 of 4 interfaces													
#	Interface	In % Utilization	Out % Utilization	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Non-Unicast/s	Out Non-Unicast/s	In Discards/s	Out Discards/s	In Errors/s	Out Errors/s
1	Se0/0/0	100.00	100.00	100.82	101.38	30,206.35	48%	32,123.05	0.00	0.00	0.00	0.00	0.00
2	Se0/0/0.1	100.00	100.00	100.72	101.28	30,204.65	48%	32,121.75	0.00	0.00	0.00	0.00	0.00
3	An1/0	0.02	0.28	4.02	109.45	2,764.15	4%	35,292.85	0.02	0.12	0.00	0.00	0.00
4	Fa0/0	0.00	0.00	0.60	0.62	138.47	<1%	140.47	0.07	0.13	0.00	0.00	0.00

Rows per page: 15 Units: Bytes/s Go to page: 1 of 1

Select an item then take an action -->

Details available on each interface:

- Top Hosts
- Top Applications
- Top Conversation Pairs

**Real-Time &
Historical
Reports Available**



Router Interface Monitoring

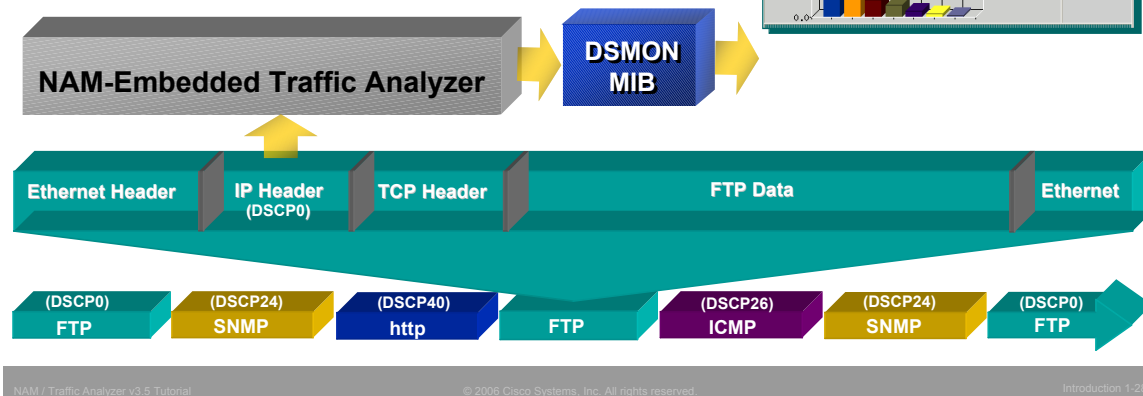
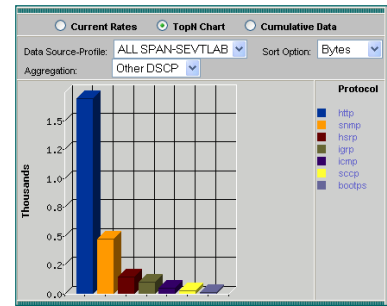
The NAM extends RMON capabilities to VLANs by implementing the Switch Monitoring (SMON) standard, a specification for monitoring switched networks. Like RMON, SMON also collects data by analyzing the headers in packets and aggregating them by VLAN ID. Utilizing SMON, the NAM offers the ability to collect and report resource utilization by VLAN and it also supports the simultaneous monitoring of multiple VLANs. With this feature, you can view traffic and priority statistics by VLAN and use this to determine if further drill down is necessary. The NAM also stores individual RMON statistics for each VLAN to support multiple management activities at any given time.

Traffic Analyzer Software

Differentiated-Services Monitoring (DS-MON)

DiffServ monitoring can be used to:

- Validate planning assumptions and QoS allocations
- Detect incorrectly marked or unauthorized traffic



DiffServ Monitoring

The NAM also incorporates Differentiated Services (DiffServ) monitoring by implementing DSMON, a DiffServ monitoring specification. An extension of the RMON methodology, DSMON looks into the IP header of every packet to identify the DiffServ code point that defines how DiffServ, enabled on devices, should handle a packet. Couple this ability with RMON packet analysis and you can see how the NAM can give you the same host, application, and conversation pair statistics for every DiffServ code point (DSCP) it observes. In essence, the NAM aggregates statistics by DSCP and it also supports grouping of DSCPs into classes of service that map onto the QoS policies that you have implemented. This enables you to fully customize how the NAM reports DiffServ statistics so that it matches your environment.

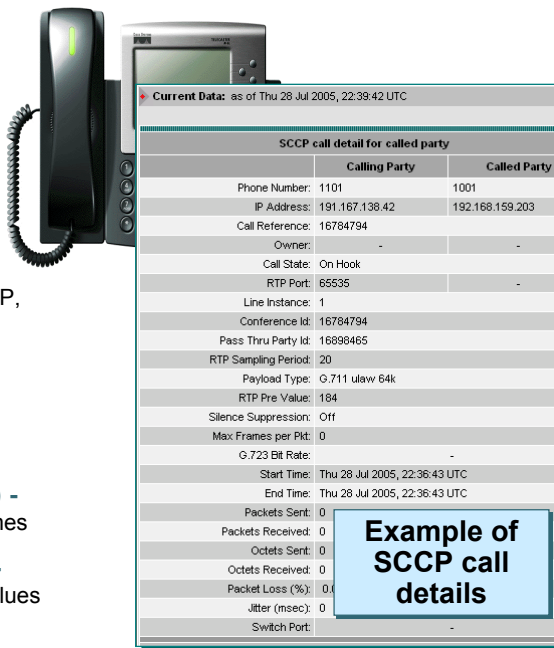
Using the NAM DiffServ monitoring capabilities, you can identify which hosts, conversations, and applications participate in each grouping of DiffServ classes. You can use this information to validate and tune your planning assumptions and QoS allocations. You can also use it to detect incorrectly marked or unauthorized traffic.

Traffic Analyzer Software

Voice Monitoring

Voice Monitoring Features

- Identify call quality degradation
 - o **Packet loss** statistics report
 - o **Jitter** statistics report
- Track active call attributes
 - o **Call Details** report
- Details for individual phones
- Protocols monitored (SCCP, H.323, MGCP, SIP, and RTP streams)



Current Data: as of Thu 28 Jul 2005, 22:39:42 UTC

SCCP call detail for called party		
	Calling Party	Called Party
Phone Number:	1101	1001
IP Address:	191.167.138.42	192.168.159.203
Call Reference:	16784794	
Owner:	-	-
Call State:	On Hook	
RTP Port:	65535	-
Line Instance:	1	
Conference Id:	16784794	
Pass Thru Party Id:	16898465	
RTP Sampling Period:	20	
Payload Type:	G.711 ulaw 64k	
RTP Pre Value:	184	
Silence Suppression:	Off	
Max Frames per Pkt:	0	
G.723 Bit Rate:	-	
Start Time:	Thu 28 Jul 2005, 22:36:43 UTC	
End Time:	Thu 28 Jul 2005, 22:36:43 UTC	
Packets Sent:	0	
Packets Received:	0	
Octets Sent:	0	
Octets Received:	0	
Packet Loss (%):	0	
Jitter (msec):	0	
Switch Port:	-	

Example of SCCP call details

Monitoring Techniques

- **RMON1 and 2** - Distribution of Voice / Video protocols
- **Application Response-Time (ART)** - Measure Cisco CallManager response times
- **Differentiated Services (DSMON)** - Monitoring voice/video traffic by DSCP values

Voice Monitoring

Integrating voice applications into a packet switched environment brings many challenges with it. As indicated earlier, voice traffic is more sensitive to variations in the delay of packet delivery and packet loss if there is significant loss. Measuring these values, packet loss and jitter, as well as visibility into the performance of your voice services is essential because users will expect the same QoS from your voice-over-IP (VoIP) services as they receive from legacy telephony systems.

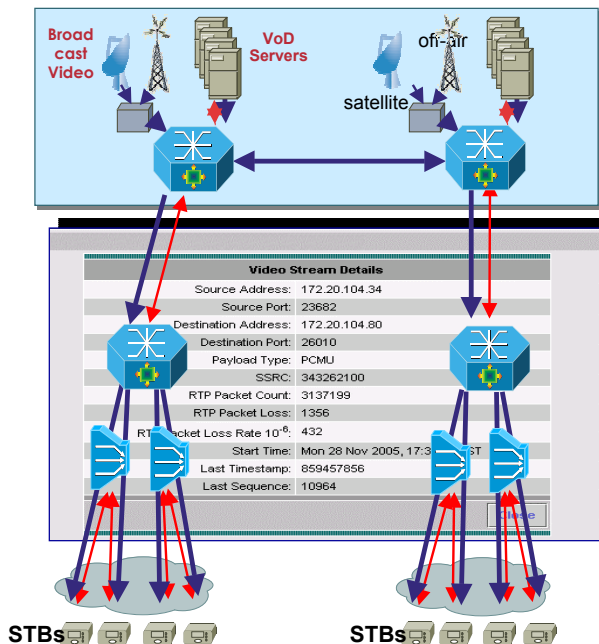
The NAM offers a wealth of data collection and analysis features to support VoIP services. Via the NAM Web interface, you can monitor active call attributes and drill down into the details of individual call records. The NAM also supports reporting on packet loss and jitter statistics for all calls, as well as for individual calls to facilitate troubleshooting. You can also configure alarms for voice traffic to generate messages when jitter and packet loss levels exceed acceptable thresholds, enabling you to proactively resolve service issues before they escalate.

Using the NAM, you can also take advantage of RMON and RMON2 statistics to gather voice protocol distribution statistics to identify VoIP utilization patterns. And you can use ART monitoring to measure the performance of the Cisco CallManager. You can also use DSMON templates to create voice profiles to monitor voice traffic for QoS violations or to ensure that voice traffic is receiving the appropriate priority you have defined for it. Using packet loss and jitter statistics along with RMON protocols statistics, application response-time monitoring, and QoS reporting gives you a powerful dataset for determining voice services trends and anticipating the infrastructure changes that will be necessary to support increased demand in voice services.

Traffic Analyzer Software

Video Monitoring

- **Proactively monitors RTP streams**
- **Filter RTP streams of interest by source / destination addresses**
- **Troubleshooting Video Broadcast issues**
 - Utilize real-time video RTP packet count and packet loss statistics
 - Receive alarms on packet loss thresholds defined
 - View RTP packet loss events logged as Syslog messages



Video Monitoring

The NAM will provide RTP packet loss statistics so that the quality of video streams for video over IP applications such as IPTV and Video on Demand can be easily and proactively observed. The goal of the NAM video stream monitoring feature is to enable the proactive analysis of video traffic to help assure a high rate of packet delivery so users and subscribers get the picture they expect and demand.

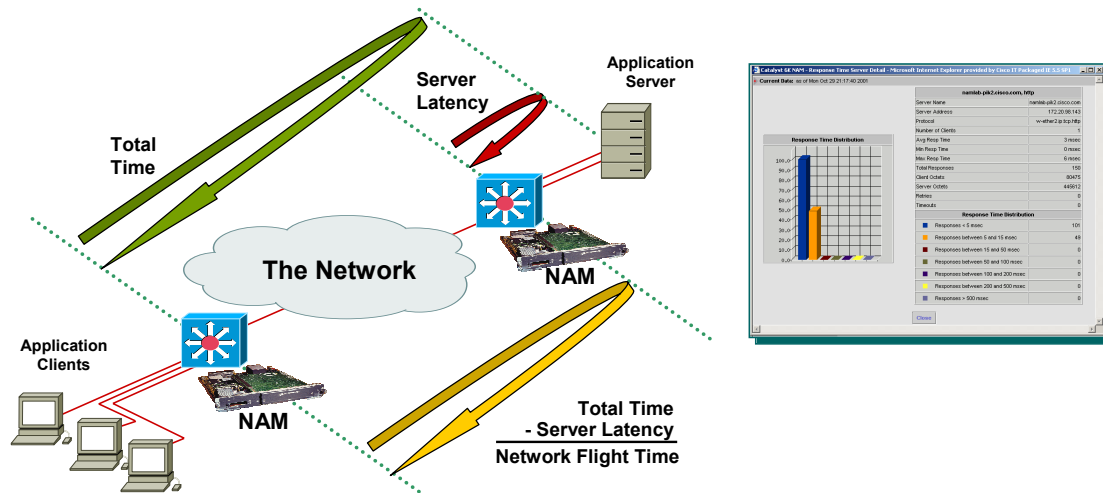
The NAM will monitor live RTP streams to detect drops to an accuracy of 10⁻⁶. These packet loss events will be recorded in a log file.

Thresholds can be defined on certain packet loss attributes and the user can be alerted when a threshold is exceeded using an SNMP trap.

Traffic Analyzer Software

Application Response Time (ART) Monitoring

Where's the latency occurring? The Network or The Application?



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction 1-31

Application Response-Time Monitoring

When the user says, “the network is slow today” or “this application is unresponsive,” where do you look to verify the user’s experience? This is a difficult question because there has been no easy way to directly relate the user’s experience to data that helps distinguish between network and application problems. Having measurements that reflect the user’s experience of network performance enables you to more quickly identify the source of performance degradation and resolve problems before users even notice. Application response-time monitoring provides these measurements and can serve as a general barometer of network performance.

By implementing ART monitoring, the NAM can collect response-time statistics on client/server requests and responses. By enabling application response-time monitoring, the NAM collects and reports response-time statistics for critical devices attached to any port or interface. In addition, response-time analysis and reporting is fully customizable, allowing you to define the time increments by which your applications and servers are measured, giving you full control over response-time reporting. You can also retrieve response-time data to collect and determine trends of this data over time. With data like this, you can correlate changes in network and application usage with fluctuations in response times to predict how changes in user populations will impact application performance. That is valuable information to have!

Traffic Analyzer Software

URL Monitoring

- Monitor hits on top URL sites
- Collect URL host, path, and content
- URL can be monitored like an application (**URL-based Application**)

This allows usage statistics to be collected

- Packet / byte rates
- Who's sending packets (Host / Conversation statistics)

- **NAM permits filtering of URL by host, path, and content**

Data Source: **Internal**

Showing 1-10 of 98 rows

	#	URL ▾	Hits
<input type="radio"/>	1	http://192.168.137.146/	1
<input type="radio"/>	2	http://192.168.137.146/admin/system/resources/overview.php	1
<input type="radio"/>	3	http://192.168.137.146/alarms/intro.php	1
<input type="radio"/>	4	http://192.168.137.146/auth/login.php	1
<input type="radio"/>	5	http://192.168.137.146/auth/logout.php	1
<input type="radio"/>	6	http://192.168.137.146/capture/intro.php	1
<input type="radio"/>	7	http://192.168.137.146/help/divva/%22+parent.relPath+%22shared/c	4
<input type="radio"/>	8	http://192.168.137.146/help/mappingfiles/divva_hlp.js	15
<input type="radio"/>	9	http://192.168.137.146/help/shared/content.css	2
<input type="radio"/>	10	http://192.168.137.146/images/akr_btn_hit_bg_08.gif	10

Rows per page:

↑-- Select an item then take an action -->

URL Monitoring

The NAM can also be configured to listen to HTTP traffic (TCP port 80) on a selected data source to collect URL information.

A URL, for example: **http://host.domain.com/intro?id=123**, consists of a host part (**host.domain.com**), a path part (**intro**), and an arguments part (**?id=123**). The collection can be configured to collect all parts or it can be configured to collect only some of the parts and ignore others.

Once the URL statistics are collected, you can view the URL and the number of hits to it. This URL collection list, illustrated above, can be filtered to look for any part of the URL, host, path, or argument.

To obtain additional statistics on the HTTP traffic, you can create an URL-based application. This allows the NAM to collect application-based statistics (packet or bytes to/from), hosts, and conversations.

Traffic Analyzer Software

Packet Capture and Decode

The screenshot displays the Traffic Analyzer Software interface. At the top, there's a status bar showing 'Loading: 1-600 of 1381' and buttons for 'Stop', 'Prev', 'Next', '1000', 'Go to', '1', 'Display Filter', and 'TCP Stream'. Below this is a table of captured packets:

Pkt	Time(s)	Size	Source	Destination	Protocol	Info
1	0.000	422	nmtq-core2-6509-NAM...	sic-vpn7-26.cisco.com	HTTP	HTTP/1.1 302 Found (text/html)
2	0.027	66	stage-2.cisco.com	54.70.163.166	TCP	2201 > microsoft-ds [SYN] Seq=992379574 A...
3	0.027	66	stage-2.cisco.com	54.70.163.166	TCP	2201 > microsoft-ds [SYN] Seq=992379574 A...
4	0.029	66	stage-2.cisco.com	54.70.163.166	TCP	2201 > microsoft-ds [SYN] Seq=992379574 A...
5	0.074	66	stage-2.cisco.com	160.59.137.88	TCP	2157 > microsoft-ds [SYN] Seq=3869079734 A...
6	0.075	66	stage-2.cisco.com	160.59.137.88	TCP	2157 > microsoft-ds [SYN] Seq=3869079734 A...
7	0.075	66	stage-2.cisco.com	160.59.137.88	TCP	2157 > microsoft-ds [SYN] Seq=3869079734 A...
8	0.077	683	sic-vpn7-26.cisco.com	nmtq-core2-6509-NAM...	HTTP	GET /capture/settingas.php?capname=Capture...
9	0.078	683	sic-vpn7-26.cisco.com	nmtq-core2-6509-NAM...	HTTP	GET /capture/settingas.php?capname=Capture...
10	0.078	64	nmtq-core2-6509-NAM...	sic-vpn7-26.cisco.com	TCP	www > 4602 [ACK] Seq=1535031187 Ack=315...

Below the table, a detailed packet decode for packet 1 is shown:

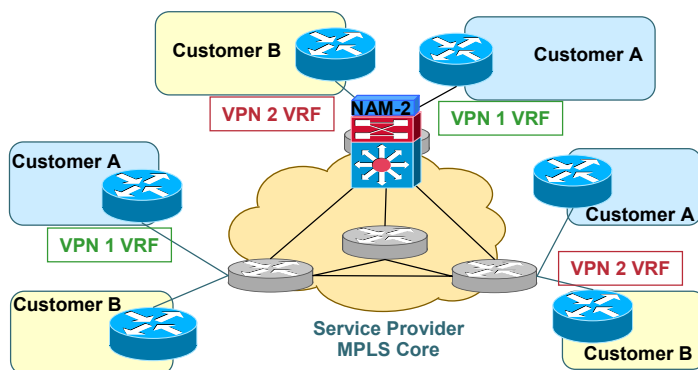
- Packet** Number: 1 - Time: Sep 11, 2006 17:11:10.318 - Packet Length: 422 bytes - Capture Length: 422 bytes
- ETH** Ethernet II, Src: Cisco 03:b8:00 (00:11:5d:03:b8:00), Dst: Cisco 31:6e:40 (00:12:da:31:6e:40)
- VLAN** 802.1Q Virtual LAN
- IP** Internet Protocol, Src: nmtq-core2-6509-NAM.localdomain (192.168.137.82), Dst: sic-vpn7-26.cisco.com (10.21.144.26)
- TCP** Transmission Control Protocol, Src Port: www (80), Dst Port: 4602 (4602), Seq: 1535031187, Ack: 3150233626, Len: 364
- HTTP** Hypertext Transfer Protocol
 - HTTP 1.1 302 Found
 - Request Version: HTTP/1.1
 - Response Code: 302
 - Date: Mon, 11 Sep 2006 17:11:10 GMT

The bottom section shows the raw packet data in hexadecimal and ASCII format.

Support Troubleshooting Efforts

Packet Capture and Decode

There may be times when you want to view the contents of packets that traverse the network, perhaps to drill down deeper into the source of a problem or just to do your own analysis. Having the ability to mirror traffic from any port on the switch or any interface on a branch router to the NAM for packet decode is an extremely convenient option. This feature comes with configuration options to optimize the collection of data to meet your needs as well as options to filter packets after you have collected the data. In addition, you can view the entire contents of a packet, all the headers as well as the data payload, in either plain text format or in hexadecimal format. You can also save your packet capture to a file in a standard format for import into utilities such as application profiling and modeling tools.



- MPLS provides an elegant solution to overlapping IP address spaces when sharing a core backbone
- Packet forwarding is done based on labels, which are assigned when the packet enters the MPLS network
- Switching is based on labels and the IP address is never looked at

The NAM:

- Learns the VRF /VCID configurations from switch using Telnet or SSH (or manually import)
- Discovers all incoming / outgoing routes via the VPN route forwarding (VRF) tables
- Monitors traffic for selected VRFs
- Reports (real-time or historical) traffic statistics, application stats, hosts, or conversations

IP / MPLS Monitoring

The overlapping addresses, usually resulting from usage of private IP addresses in customer networks, are one of the major obstacles to successful deployment of peer-to-peer VPN implementations. The MPLS/VPN technology provides an elegant solution to the dilemma.

Multi-protocol Label Switching (MPLS) combines the benefits of layer 2 switching with layer 3 routing and switching. This new technology results in simpler customer routing and simpler service provider provisioning, and makes possible a number of topologies that are hard to implement (overlay or peer-to-peer VPN models). MPLS also adds the benefits of a connection-oriented approach to the IP routing paradigm, through the establishment of label-switched paths, which are created based on topology information rather than traffic flow.

A NAM placed in the network can be used to monitor traffic embedded in the MPLS packets! By communicating with the switch using Telnet or SSH, the NAM can learn the VRF / VCID configurations or the administrator can import them manually using the NAM's user interface. The NAM can then monitor and discover the VPN route forwarding tables.

Once the mapping is known, the NAM can collect statistics per VRF name. All RMON2 statistics and extensions are available for the entire data source or per VLAN/MPLS VRF, VCID, or Label within the Data Source. Thus, upper layer statistics can be enabled to allow for monitoring of hosts, conversations, and applications. Additionally, packet capture and decode can be performed and application response times can be measured on the MPLS traffic streams.

Traffic Analyzer Software

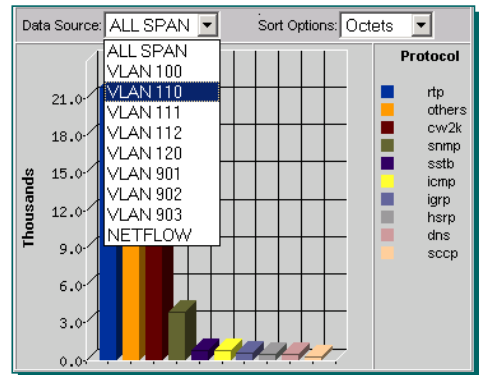
VLAN Monitoring

**Catalyst 6500 and Cisco
7600 Series NAM 1/2 only**

VLAN Traffic Statistics by Individual VLAN

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data				
VLAN ID	Packets/s	Bytes/s	Non-Unicast Pkts/s	Non-Unicast Bytes/s
1. 99	53.60	7753.94	4.57	320.34
2. 100	79.00	13423.93	10.70	924.48
3. 110	4.54	528.14	3.76	258.41
4. 130	4.34	301.20	4.13	283.59
5. 140	3.78	271.69	3.61	248.48
6. 200	4.20	318.28	2.92	204.39
7. 901	3.61	249.06	3.59	246.60

Application Monitoring per Spanned VLAN



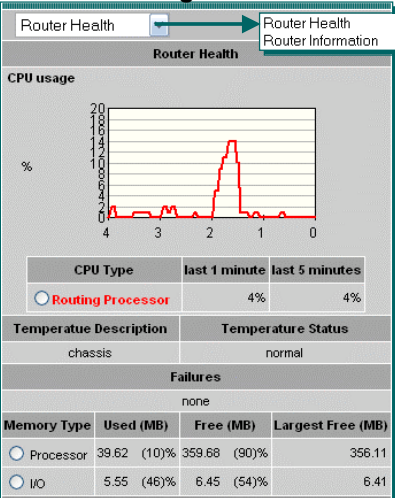
VLAN Monitoring

The NAM extends RMON capabilities to VLANs by implementing the Switch Monitoring (SMON) standard, a specification for monitoring switched networks. Like RMON, SMON also collects data by analyzing the headers in packets and aggregating them by VLAN ID. Utilizing SMON, the NAM offers the ability to collect and report resource utilization by VLAN and it also supports the simultaneous monitoring of multiple VLANs. With this feature, you can view traffic and priority statistics by VLAN and use this to determine if further drill down is necessary. The NAM also stores individual RMON statistics for each VLAN to support multiple management activities at any given time.

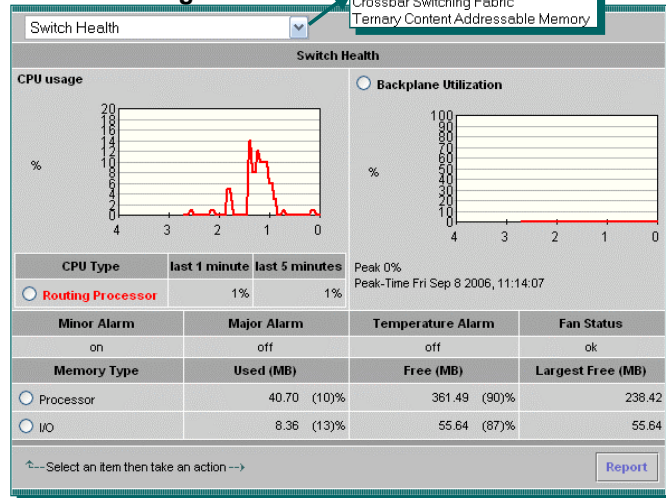
Traffic Analyzer Software

Overall System Health

Router Hosting NM-NAM



Switch Hosting NAM-1/2



Tight integration with the switch/router permits the NAM to monitor and track important infrastructure health diagnostics

Overall System Health

As with all critical network devices, monitoring the overall health of a switch or router is important for keeping traffic flowing through the network and monitoring the impact to network devices when deploying new application services.

When the Traffic Analyzer health report is run, the NAM will retrieve vital performance statistics from the device hosting the NAM and display them. Monitor vital resources such as:

- CPU utilization
- Backplane bandwidth
- Memory usage
- Temperature and fan status
- SysUpTime
- Power supply status

Besides Switch Health, the NAM-1/2 also includes health-based reports covering Switch Information, Crossbar Switching Fabric, and Ternary Content Addressable Memory.

Also, the NM-NAM also includes health-based reports covering Router Information.

CISCO SYSTEMS



Network Performance Monitoring

Network Analysis Modules

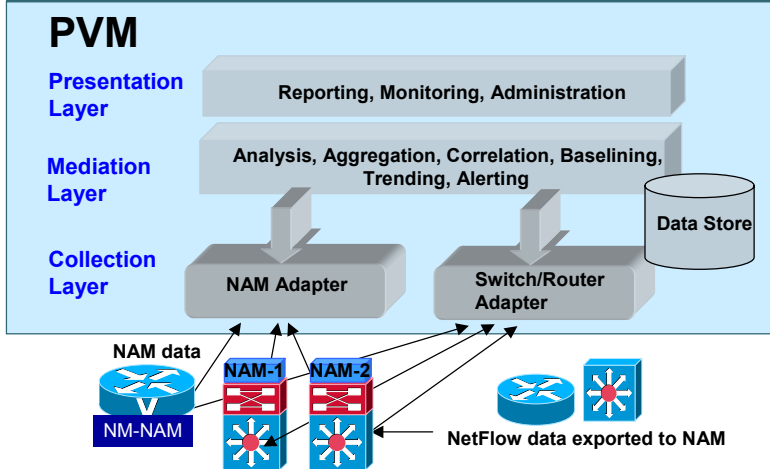
Traffic Analysis Software

Cisco Complementary Solutions



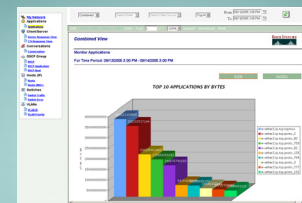
Cisco Complementary Solutions

Performance Visibility Manager (PVM)



- Centralized configuration and control of data sources
- Aggregated views and reports from multiple data sources
- Proactive alerting
- Strong reporting
- Web-based client
- API and integration

“Better visibility means better business decision, increases network availability and customer satisfaction”



Cisco Complementary Solutions – Performance Visibility Manager (PVM)

Cisco Performance Visibility Manager (PVM) is a proactive network- and application-performance monitoring, reporting, and troubleshooting system for maximizing network availability. It increases early visibility into network and application behavior issues, to identify them before they become critical.

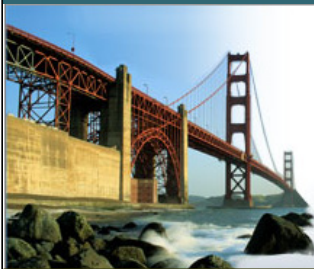
PVM offers:

- Traffic analysis capabilities to give visibility into the network and business applications, allowing network managers to understand how application traffic effects network performance and preventing misuse of critical network resources.
- An application response time (ART) monitoring capability to immediately identify whether or not poor application performance is being caused by the network or the application.
- An intuitive GUI that presents a high-level operational view to quickly pinpoint trouble spots and provide a mechanism to easily navigate to the next level of detail for further troubleshooting. The historical viewing capability allows network managers to discern what is happening in real time with historical analysis of past events.
- An automatic baseline module to help proactively manage problems by continuously monitoring for conditions that may represent an emerging problem, facilitating early detection of potential performance issues.
- Comprehensive reports that assist network managers in capacity planning, trending analysis, and ongoing status monitoring.

As illustrated above, support for traffic and ART data from multiple sources including Cisco Network Analysis Module (NAM), network devices, and others.

Cisco Complementary Solutions

NAPA Solution



Bridge the Gap

Network Application Performance Analysis

Monitor, Analyze, and
Optimize Your Network

Utilizing a comprehensive bundled toolset and expertise from Cisco Consulting Engineers, achieve:

- Better network performance
- Faster identification and resolution of problems
- Significantly enhanced network planning capabilities
- Reduced risk
- Access to Cisco advanced services
- Greater efficiency, productivity, and profitability

Bundled Solution of Tools & Services

- *Cisco Network Planning Solution*
- *Cisco Application Analysis Solution*
- *CiscoWorks Resource Manager Essentials*
- *Cisco NAMs*
- *Cisco Performance Visibility Manager*
- *Cisco NetFlow Collection Engine*
- *Cisco Advanced Services provide expertise on planning, toolsets, protocols, and application usage*
- *Software Upgrades and Support*

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction 1-39

Cisco Complementary Solutions – NAPA Solution

The Network Application Performance Analysis (NAPA) Solution is a comprehensive set of tools and services that provides information about application and network performance.

The Cisco NAPA Solution provides valuable information about the performance of the network and the applications running on it. With the Cisco NAPA Solution, when a problem arises, users can identify whether it's related to the network, servers, or applications. Once the problem is diagnosed, the Cisco NAPA Solution provides the insight required to fix it.

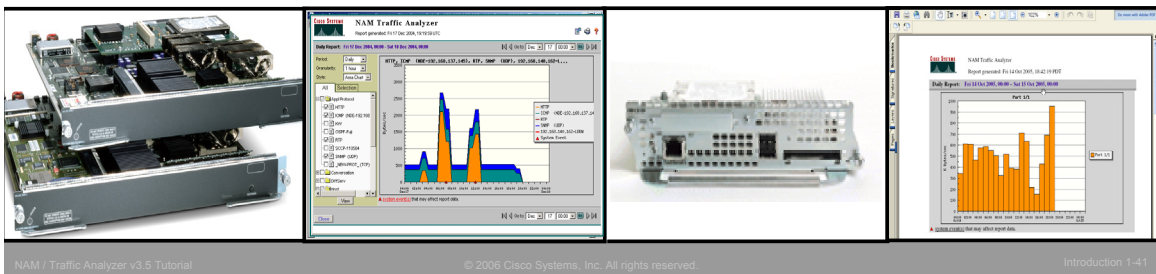
The Cisco NAPA Solution also helps with predictive planning and optimization for successful deployment of new applications and network services. By modeling network scenarios, the Cisco NAPA Solution reduces the risks associated with new network deployments.

As illustrated above, the Cisco NAPA Solution is not just a comprehensive, integrated set of tools. It also is comprised of professional services designed to optimize performance and streamline troubleshooting of your applications and network.

This page intentionally left blank.

Summary: Benefits Achieved

- Using the NAM provides 'Visibility' into your network from *within* your network
- Be proactive and make the right decisions
 - Make accurate business decisions about your IT resources
 - Identifies traffic with greatest impacts to performance
 - Pinpoint latencies and isolate problems
- "Right-size" the network to reduce network spending \$\$



Summary: Benefits Achieved

For most users they do not care about how they get the data, just that they get it. However, improperly managed networks lead to downtime and loss of access to important data making users painfully aware that their data depends on a network. Of course, every little glitch will now be blamed on the network amplifying the need for network monitoring.

And here with performance monitoring, the key to decision making will be the visibility within the network. A well thought out and implemented network management strategy provides users with a consistent high-level of network services increasing productivity. The collected management data also can be used to maximize ROI (return on investment), verify third party service agreements, quantify change and growth leading to an overall increase in network reliability and effectiveness, and not to mention saving lots of money.

Thank You!

Chapter 1 provided you with a quick overview of the need for network performance monitoring and Cisco's solution – the NAMs for both the Cisco Catalyst 6500 and Cisco 7600 series routers as well as the Cisco Branch Routers Series. The NAMs provide a wealth of information with the integrated Traffic Analyzer software.

Now, continue on to Chapter 2 to discover how to set up and use NAM to provide access to a rich set of traffic statistics collected by the NAM.



Product Features

Chapter 2

- **Cisco Network Analysis Modules (NAM)
NAM-1, NAM-2, and the NM-NAM**
- **Cisco NAM Traffic Analyzer Software v3.5**



Chapter 2 Outline

- **Network Monitoring Using NAMs**
- **NAM Hardware Overview**
 - Cisco Catalyst 6500 Series and Cisco 7600 Series NAM-1, NAM-2
 - Cisco Branch Routers Series NM-NAM
- **Traffic Analyzer Software**
 - Planning
 - Getting Started
 - Configuring
 - Viewing Reports
 - Packet Capture and Decode



Chapter 2 Outline

Hopefully, Chapter 1 introduced the need and benefit of having visibility into the packet streams traversing the network. In this chapter, we re-introduce the Network Analysis Module (NAM) as a powerful integrated network monitoring tool designed to give network managers more visibility into their network than ever before. The innovative design of the NAM combines Simple Network Management Protocol (SNMP) agent functionality with a Web-based management console, all of which resides on a single blade in the Cisco 6000 series Catalyst switch or Cisco Branch Router series. The NAM architecture combines standard SNMP agent features with full Remote Monitoring (RMON) 1 and 2 collection as well as other Management Information Bases (MIBs) such as Application Response Time Monitoring (ART), virtual LAN (VLAN) Switch Monitoring (SMON), Differentiated Services Monitoring (DSMON), Voice over IP (VoIP), and Network-Based Application Recognition – Protocol Discovery (NBAR-PD) to provide more comprehensive instrumentation of voice and data networks. By implementing this functionality in supported switches and routers, Cisco offers you visibility into your network end to end through all seven layers of the Open System Interconnection (OSI) protocol stack.

This section is based on the features found in the integrated NAM Traffic Analysis Software v3.5 which can run on all models of NAM hardware (WS-SVC-NAM-1, WS-SVC-NAM-2, and NM-NAM).

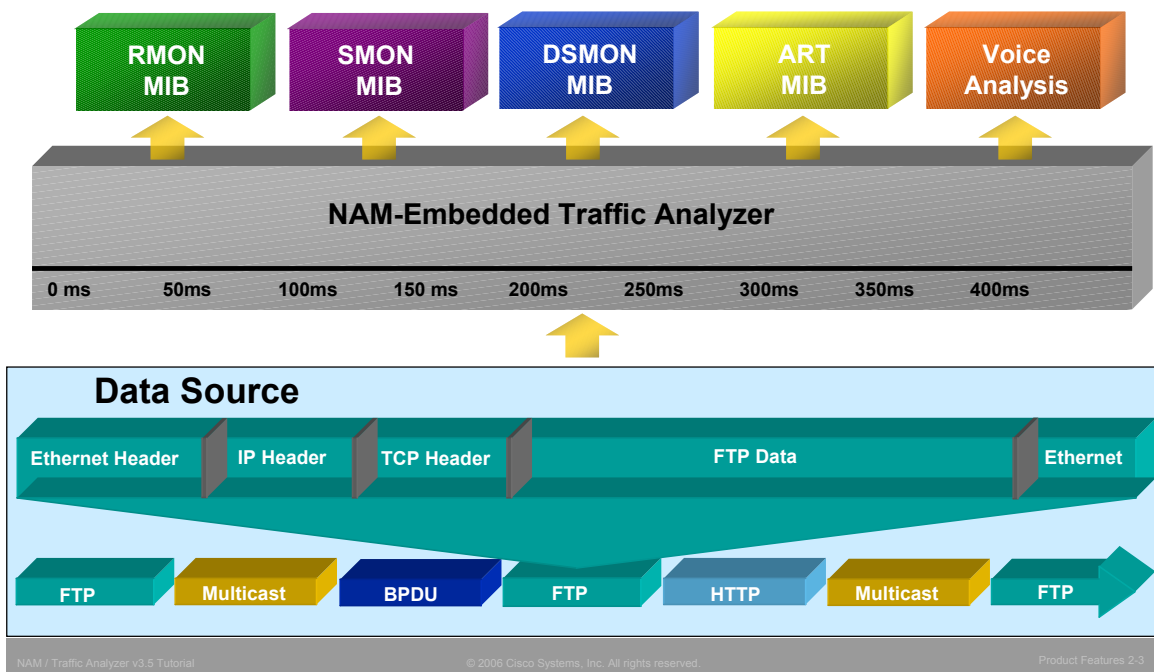
Please note that this chapter does not cover all configuration options of the NAM. Refer to the NAM User Guide for more details on configuring the NAM to meet your specific needs. If you intend to use this tutorial as a primer for the actual use of the NAM, Cisco recommends that you first install the product so that you can follow along. Refer to Chapter 3 for deployment scenarios that offer NAM solutions to real-world problems, Chapter 4 for installation tips, and the NAM Installation Guide for step-by-step installation instructions. (Links to the NAM Installation and User Guides can be found in Chapter 5.)

Note(s):

- *Cisco Catalyst® 6500 and Cisco 7600 Series Network Analysis Modules will be referred to, in this tutorial, as the Cat6500 NAM(s), NAM-1, NAM-2 or NAM-1/2.*
- *Cisco Branch Routers Series NAM will be referred to, in this tutorial, as the NM-NAM.*
- *The term NAM refers to all modules, NAM-1, NAM-2, and the NM-NAM.*

Network Monitoring Using NAMs

Overview



The Data the NAM Collects

What does the NAM collect? All the wealth in network analysis is contained in the packets that traverse the network, and information about the packets are what the NAM collects. This offers us the benefit of seeing and measuring traffic by the smallest details stored in the packets—its Layer 2, 3, and 4 headers—and where it can also be measured by time. Capturing data at the source, the switch, also enables us to see the participation of each packet in network activities, such as VLANs, MPLS, and voice calls.

However, the ability to collect packet information at the source alone does not give us the ability to analyze it from different perspectives, those of VLANs, voice, or quality of service. Those abilities have been added through the implementation of standard and proprietary monitoring specifications such as RMON, SMON, ART MIB, DSMON, and Detailed Call Records. These MIBs and VoIP constructs enable us to analyze the packets through the “eyes” that these MIBs offer, giving us more ways to look at each packet. As you can see, the ability to monitor your network is expanded considerably when you can monitor at the source combined with powerful analysis capabilities.

The various reports created by the NAM Traffic Analyzer software will be detailed and explained later in this chapter when describing the use of the Traffic Analysis software.

Network Monitoring Using NAMs

NAM Data Sources

NAM Data Sources

The NAM makes use of multiple data sources to provide the ultimate visibility into the network. Data sources include: mini-RMON for per-switch port layer-two statistics, Spanning, VACLs, and Cisco Express Forwarding (CEF) to copy actual packets traversing the switch fabric and router interfaces to the NAM for analysis, MIB-II for per-router interface statistics, NBAR statistics for protocol information on a per interface basis, and NetFlow to provide application, host, and conversation information from a number of remote and local traffic flows. More details on data sources used by the different NAMs will be presented in the next section of this chapter.

The user should keep in mind a number of factors when using the various NAM data sources. In some SPAN configurations, multiple copies of the same source packet can be sent to the SPAN destination port. For example, a bi-directional (both transmit and receive) SPAN session is configured for sources a1 and a2 to a destination port d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination port d1; both packets would be the same (if a Layer 3 rewrite occurs, the packets are different). Similarly, for RSPAN sessions with sources distributed in multiple switches, the destination ports might forward multiple copies of the same packet. The same is true for VLANs, if a packet is both sent and received by two ports that are part of the same VLAN they will be counted twice. To avoid counting packets twice with VLANs, the default direction for spanning VLANs is set to receive only. The two data ports available with a NAM-2 can also be used effectively to monitor the receive direction on one data port and the transmit direction on the other. Similarly, if CEF is forwarding packets from all router interfaces then the packet will be seen twice – once on the ingress interface and once on the egress interface. Again, we stress the importance of understanding the exact nature of data source in order to properly interpret the Traffic Analysis reports.

Note:

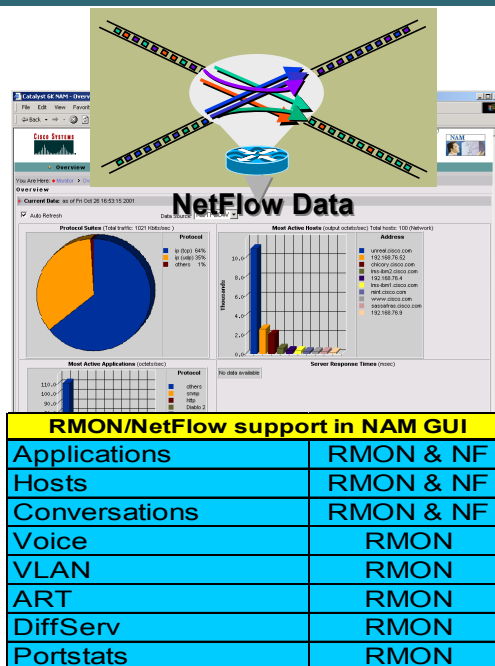
- *The NBAR MIB has not yet been implemented within the Cisco Catalyst 6500 switch and Cisco 7600 router. When these devices include support for the NBAR MIB, the Cisco Catalyst 6500 Series and Cisco 7600 Series NAM will support NBAR-PD on those devices as well.*

Network Monitoring Using NAMs

NetFlow as a Data Source

NAM offers a powerful combination of NetFlow and RMON monitoring

- Use both RMON and NetFlow to provide application-level visibility
- Exporting of NetFlow data to the NAM allows monitoring of multi-layer switched traffic (L3) on an aggregate basis
- Use the NAM RMON capability for detailed analysis of voice traffic, quality of service, application response time, and packet capture and decode



NetFlow as a Data Source

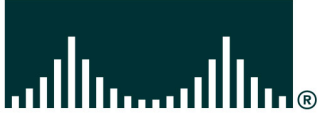
For flexibility, NetFlow data collections can be used to provide coverage of streams not directly accessed by the NAM. Hence, an important WAN interface that you wish to monitor but the host router cannot accept a NAM, can be analyzed by enabling NetFlow for the interface and exporting the collection statistics to a NAM.

The NAM provides a more in-depth analysis of the traffic streams than what NetFlow can provide. NetFlow analysis does, however, provides application visibility by reporting statistics on application usage including hosts and conversation information for each application.

Before looking at details of the NAM Traffic Analyzer software, let's first take a look at the different types of NAMs and the data source used by each.

This page intentionally left blank.

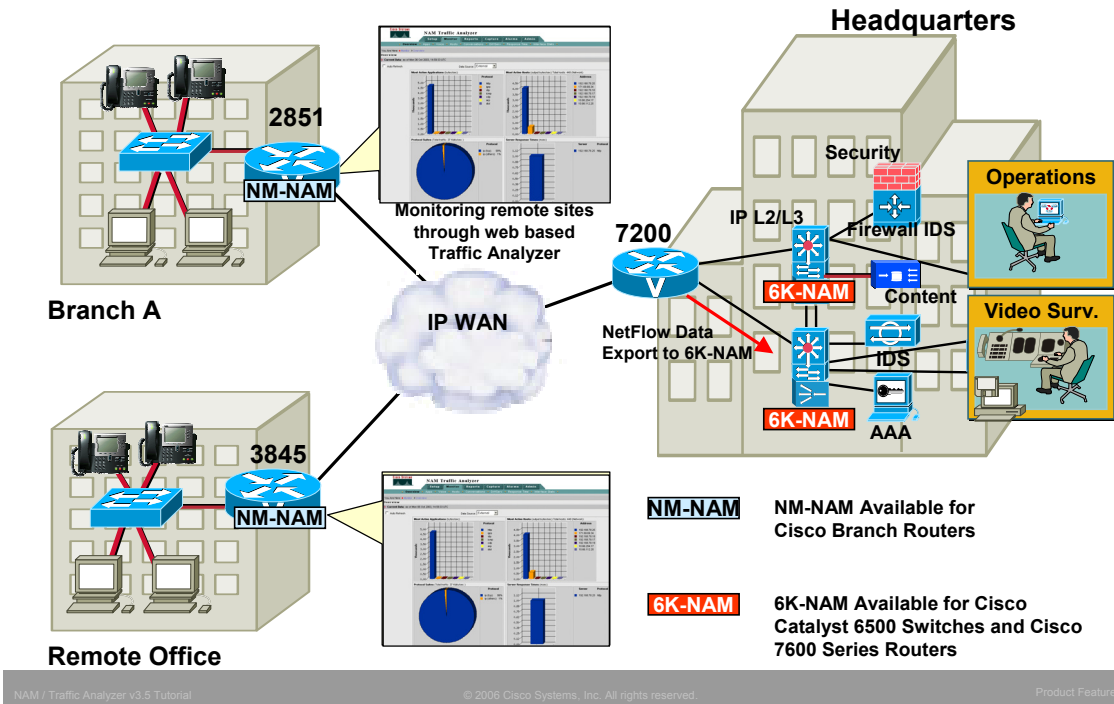
CISCO SYSTEMS



- Network Monitoring Using NAMs
- **NAM Hardware Overview**
 - **Catalyst 6500 and Cisco 7600 Series NAM-1, NAM-2**
 - **Cisco Branch Routers Series NM-NAM**
- Traffic Analyzer Software



NAMs in the Enterprise



NAM in the Network

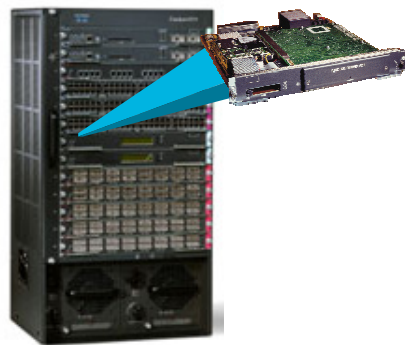
We can all agree to the importance of having traffic visibility throughout the enterprise. Therefore, the NAM comes in two basic models that allows for flexibility in monitoring. The NAM-1 and NAM-2 (number refers to the number of data ports available for monitoring data streams) are available for use in Catalyst 6500 switches and 7600 internet routers. As will be discussed in more detail shortly, these NAMs use Spanning technology to forward LAN data streams for analysis and VACL and NetFlow technology to analyze WAN data streams. The NM-NAM is available for Cisco 2600XM, 2800, 3660, 3700, 3800 Series Branch Routers utilizing Cisco Express Forwarding (CEF) and NetFlow to analyze mainly WAN data streams though it is also possible to use the NM_NAM to analyze LAN data streams.

Next we will look at details of the NAM-1 and NAM-2 sometimes referred to as the 6k-NAM.

NAM-1/2 Overview

Features

- **Multiple Data Sources for Analysis**
 - SPAN / RSPAN / ERSPAN / VACL / NetFlow
 - Supervisor module (mini-RMON, VLAN stats)
- **MIBs for storing statistics on data sources**
 - Full RMON 2 Capability
 - Hosts statistics –Network Layer
 - Conversation statistics –Network Layer
 - Upper layer protocol distribution
 - MIB Extensions
 - ART (Application Response Time)
 - DS-MON (Differentiated Services)
 - Voice / Video



RMON2 stats available for entire Data Source or per VLAN/MPLS VRF, VCID, or Label within the Data Source

NAM-1/2 Features

The NAM-1 and NAM-2 occupy a single slot (except the Supervisor slot) in the chassis of Cisco® Catalyst® 6500 Series switches and Cisco 7600 Series routers. Once inserted into the host chassis, traffic from the local switch can be copied (spanned) to the NAM for detailed analysis. The NAM effectively becomes a SPAN port.

What is RSPAN?

A user often has a need to analyze traffic flows captured by SPAN on a box different from where they are captured. Switches that support Remote SPAN (RSPAN) allow the user to capture the monitored traffic and transmit it to a remote switch that has an embedded NAM, using RSPAN VLAN.

What is ERSPAN?

However, RSPAN suffers from a limitation that the traffic cannot be analyzed on a different L2 domain from where it is sourced. Also, the L2 domain should be confined to Cisco switches due to special properties of RSPAN VLAN that are supported by Cisco switches only. ERSPAN (encapsulated SPAN) provides a solution to this problem. The ERSPAN feature allows the user to capture traffic and encapsulate it in a GRE/IP packet. This encapsulated packet can then be sent through any L3 network as a GRE tunneled packet.

Other Features

For increased flexibility, VACL can be used in place of a SPAN session as the data stream source. The NAM-2 includes a second SPAN destination to allow for increased monitoring capabilities. NetFlow can also be used as an independent data source (does not limit the use of SPAN or VACL).

Included with the NAMs is an embedded, Web-based Traffic Analyzer, which provides full-scale remote monitoring and troubleshooting accessible through a Web browser. Analysis is done through the use of many different MIBs including RMON, ART (Application Response Time), DS-MON (Differentiated Services), and VoIP (Voice over IP).

Using the integrated NAM solution, Network Managers gain valuable insight into their networks with both real-time and historical application usage for performance monitoring and trending, network planning, fault isolation, and troubleshooting purposes.

NAM-1/2 Hardware Overview Specifications

	NAM-1 WS-SVC-NAM-1	NAM-2 WS-SVC-NAM-2
SPECIFICATIONS		
• Fabric and Bus Support	Yes	Yes
• Processor	Dual	Dual + Accelerator
• RAM	512 MB	1 GB
• Hard Disk	20 GB	20 GB
• Capture Buffer	125 MB	300 MB
• Performance	Sub-gigabit	Gigabit
MONITORING APPLICATIONS	Fast Ethernet, Low capacity GE	High Capacity GE
• No. of SPAN / VACL Sessions	1	2
• No. of NetFlow Sessions	1	1
• No. of ERSPAN Sessions	1	1
DEPLOYMENT SCENARIOS	Distribution, Access, small core, Branch office	Core, Server farm, Data Center

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-10

NAM-1/2 Specifications

The chart above shows basic specifications for the NAM-1 and NAM-2 hardware. Because the NAM-2 has a second data port for receiving a second data stream for analysis it is considered the choice for high performance applications. The NAM-1 can not be upgraded to a NAM-2.

Hardware Architecture for Cisco NAM-1

High-performance, dual-processor architecture, 512 MB RAM

Two data-collection interfaces to backplane (one for SPAN and VACL data sources, one for NetFlow)

Fabric-enabled platform with interface to both bus and crossbar-based architectures

Hardware Architecture for Cisco NAM-2

Extra high-performance, dual-processor architecture with hardware-based packet acceleration, 1GB RAM

Gigabit monitoring performance

Three data-collection interfaces to backplane (two for SPAN and VACL data sources that can be used independently or together, and one for NetFlow)

Fabric-enabled platform with interface to both bus and crossbar-based architectures

Supported Platforms

Cisco NAM-1 and NAM-2 can be deployed in any slot (except the Supervisor slot) in Cisco Catalyst 6500 and Catalyst 6000 Series switches and Cisco 7600 Series routers [both bus- and crossbar (fabric)-based architectures]; multiple NAMs can be placed in the same chassis

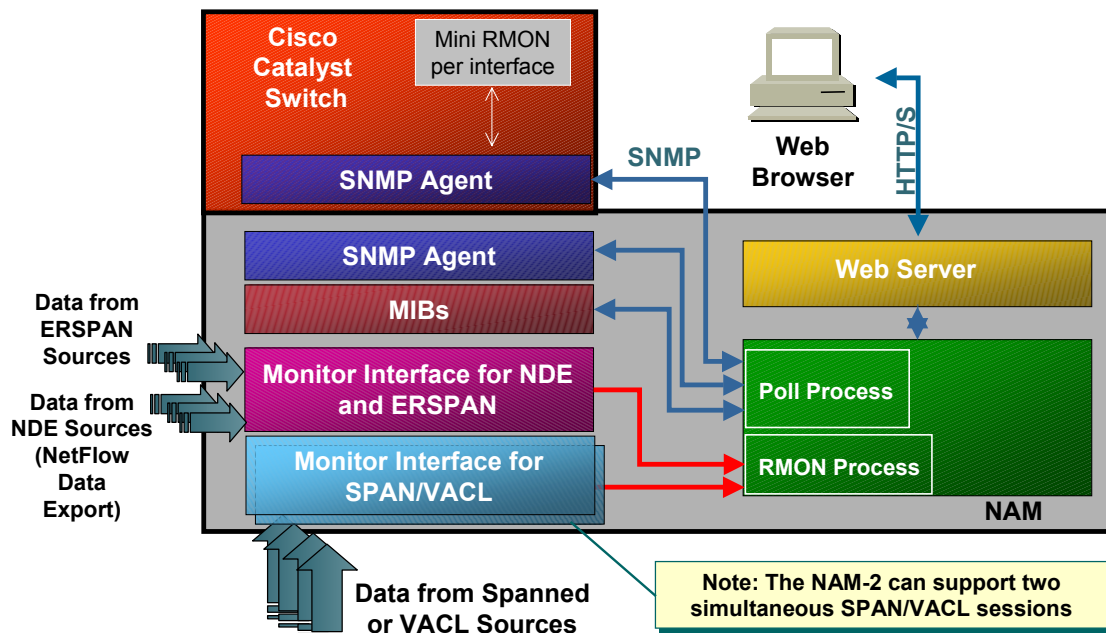
Supported with Cisco IOS® Software or Cisco Catalyst Operating System on the supervisor engine

Supported Topologies and Data Sources

LAN-Switch Port Analyzer (SPAN), Remote SPAN (RSPAN), Encapsulated SPAN (ERSPAN), VLAN ACL (VACL)-based captures, NetFlow (versions 1, 5, 6, 7, 8, and 9)

WAN-NetFlow (versions 1, 5, 6, 7, 8, and 9) from local and remote devices, VACL-based captures for FlexWAN and Optical Service Module (OSM) interfaces (Cisco IOS Software only)

NAM-1/2 Hardware Overview Architecture



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-11

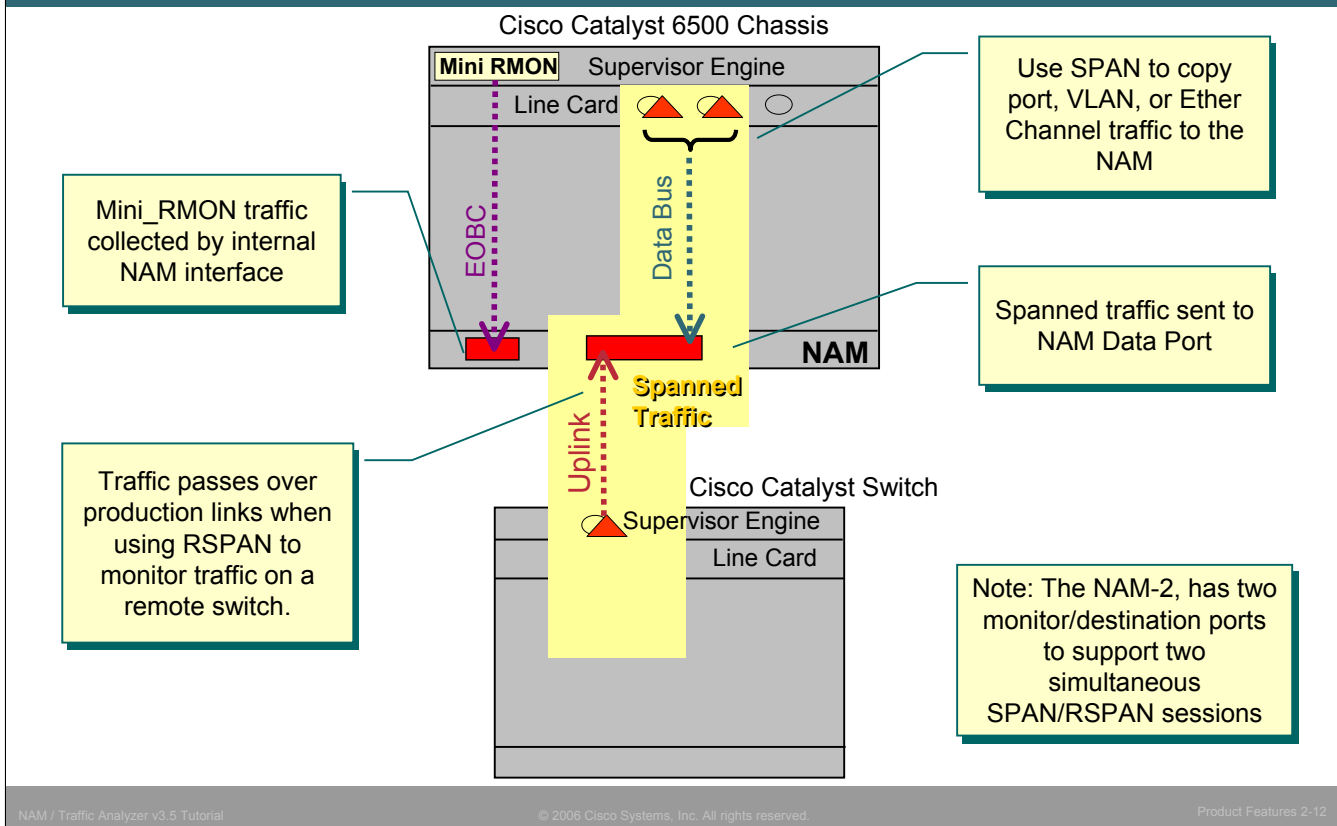
NAM-1/2 Architecture

How does data flow through the various processes in the NAM? Data enters the NAM for analysis via one of three internal interfaces on the NAM (two for monitoring), the monitor interface for NDE, the monitor interface for SPAN/VACL (two of these on the NAM-2), and the host switch SNMP agent. The data, received in frame format, is parsed by the RMON process on the NAM and stored in the RMON, SMON, and other MIBs loaded onto the NAM. The polling process grabs data from these MIBs as well as the mini-RMON MIB on the Cisco Catalyst switch and performs the data analysis and presentation functions that generate the graphical tables and charts that you see. The Web server responds to Hypertext Transfer Protocol (HTTP) requests from a client's Web browser and presents the traffic reports and the configuration menus. Together, these functions constitute the embedded "Traffic Analyzer." This tutorial is based on integrated NAM Traffic Analyzer Software v3.5.

As the figure above illustrates, the SNMP agent in both the NAM and the Cisco Catalyst switch will also respond to SNMP queries from third-party network management systems for MIB data that the NAM and Cisco Catalyst switch stores.

NAM-1/2 Data Sources

Mini-RMON / SPAN / RSPAN



NAM-1/2 Data Sources – Mini-RMON / SPAN / RSPAN

How is data sent to the NAM for collection and analysis? Well, as mentioned in the previous slide, the NAM receives data from three internal interfaces. The first is an interface used to gather mini-RMON statistics from each of the enabled ports on the host device. This allows the user to view basic layer two statistics for each port and is used to decide if further analysis is necessary for any of the ports. If further analysis is deemed necessary, the NAM analyzes actual traffic passed to it using the SPAN or VACL mechanism of the Catalyst switch.

Spanning is the term used to define the configuration required to copy traffic from source port(s), VLANs, or Cisco Ether Channel® tunnel to a destination switch port (SPAN port) for analysis. A SPAN session is an association of a *destination* monitor port with one or more *sources* of traffic. Sources can be physical ports, VLANs, or a Cisco Ether Channel tunnel. When the NAM is installed, the host switch recognizes it as a SPAN destination. The user selects one or more ports, VLANs, or Ether Channels and the switch copies the traffic from the selected sources to the NAM for analysis and reporting.

Note: the NAM-2 hardware includes two destinations to allow increased flexibility for network monitoring.

The ability to SPAN VLANs allows the user to achieve additional monitoring flexibility. Remote switches can be configured to “export” data on a special user defined VLAN. The NAM can then span this “remote” VLAN, effectively spanning data from a remote switch. This capability is known as RSPAN (Remote SPAN).

Note: RSPAN data traverses production links, this additional traffic may have an adverse performance impact on your network. Please consider these implications before implementing remote monitoring using RSPAN.

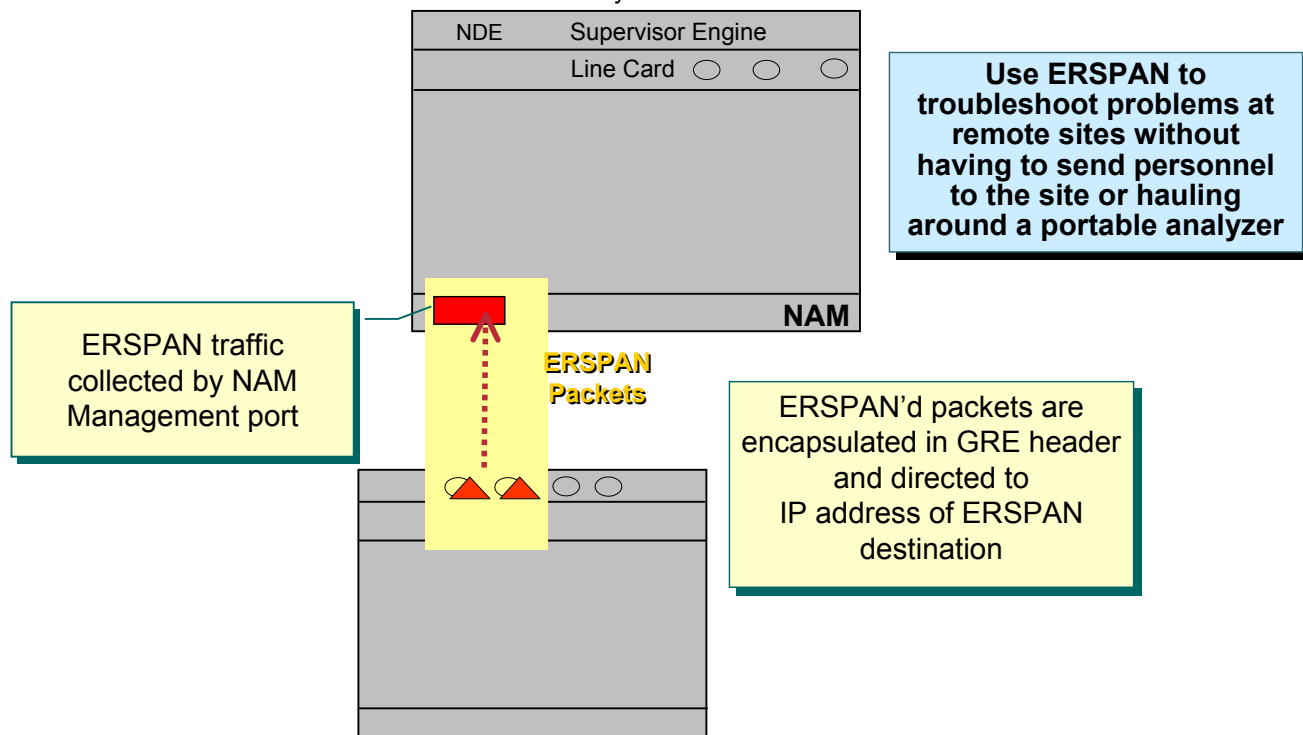
Note: RSPAN and SPAN are mutually exclusive; if using RSPAN then you will lose the ability to SPAN data to that port. Consider using a NAM-2 with its second data port to allow the NAM to do both SPAN and RSPAN together.

For further information, refer to Chapter 5 for links to additional information on SPAN and RSPAN.

NAM-1/2 Data Sources

ERSPAN

Cisco Catalyst 6500 Chassis



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-13

NAM Data Sources – ERSPAN

As discussed earlier, a user often has a need to analyze traffic flows captured by SPAN on a box different from where they are captured. Switches that support Remote SPAN (RSPAN) allow the user to capture the monitored traffic and transmit it to a remote switch that has an embedded NAM, using a RSPAN VLAN. However, RSPAN analyzes traffic only on the same L2 domain from where it is sourced. Also, the L2 domain is confined to Cisco switches due to special properties of the RSPAN VLAN that are supported by Cisco switches only.

ERSPAN (encapsulated SPAN) provides a solution to the limitations just described. The ERSPAN feature allows the user to capture traffic and encapsulate it in a GRE/IP packet. This encapsulated packet can then be sent through any L3 network as a GRE tunneled packet.

ERSPAN increases the NAM's deployment flexibility, enabling it to monitor traffic from remote parts of the network. The NAM can receive ERSPAN traffic through the internal management port (same used by NetFlow traffic). Alternatively, the ERSPAN traffic can be directed to the switch, and then the receiving port can be SPANned to the NAM for analysis.

ERSPAN traffic sent directly to the NAM is treated as a separate data source independent of the SPANned traffic. ERSPAN is supported on Sup720 with IOS 12.2(18)SXE or later and PFC3B.

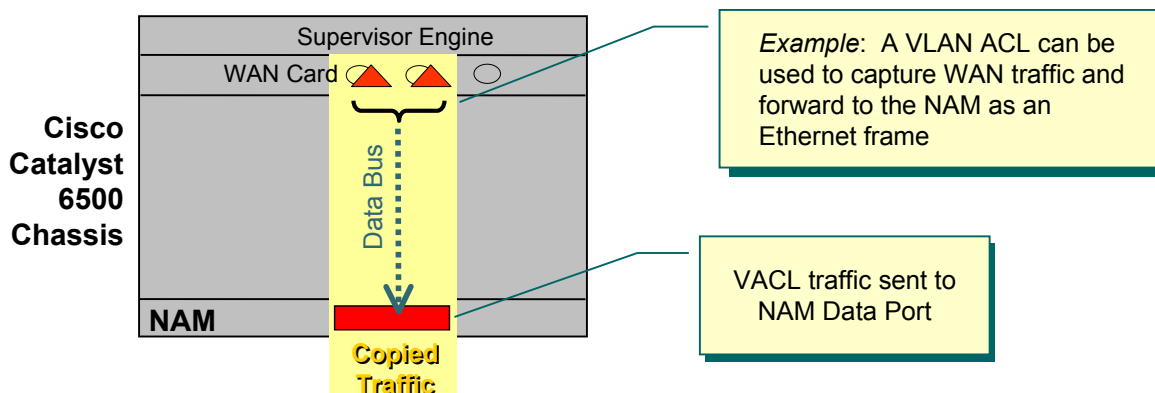
Note:

- Sending excessive ERSPAN traffic directly to NAM will slow GUI response time.

NAM-1/2 Data Sources

VACL

- **Multiple Uses of VLAN ACLs for Traffic Analysis**
 - Use a VACL to analyze WAN interfaces that can not be spanned
 - Use a VACL if no more SPAN sessions are available for use
 - Use a VACL to pre-filter specific types of traffic for analysis
- **VACL traffic sent to NAM data port looks just like SPAN data to the NAM**



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-14

NAM-1/2 Data Sources - VACL

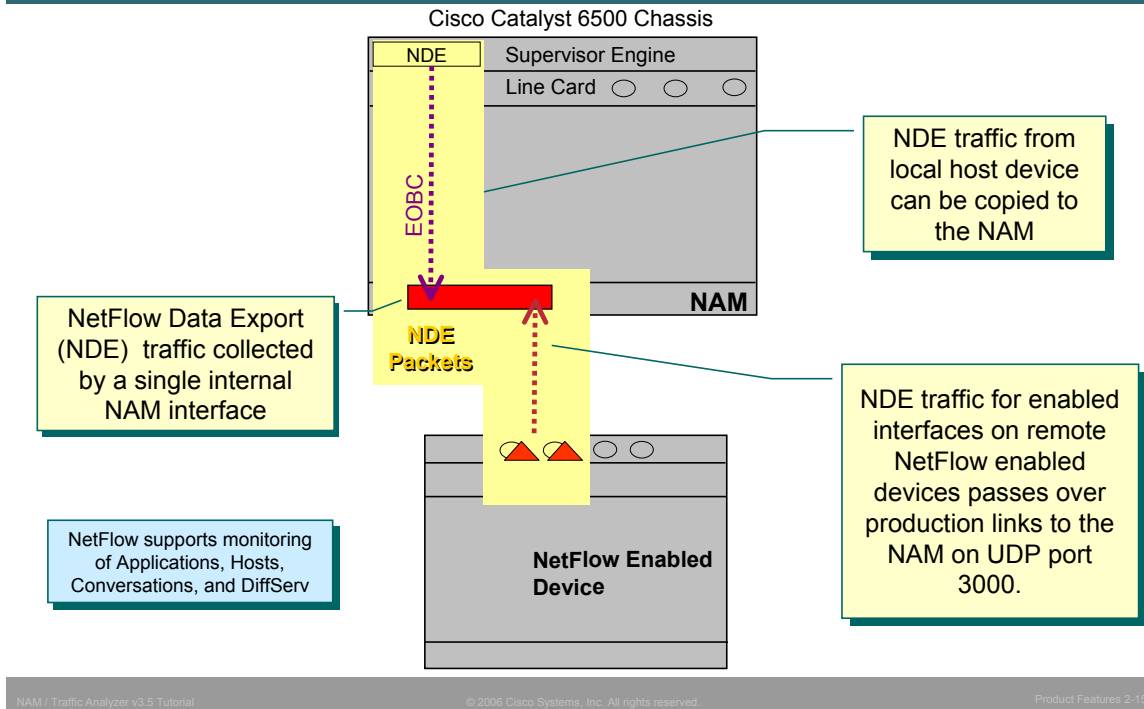
VLAN Access Control Lists or VACLs can be a valuable source of traffic for analysis by the NAM for the Catalyst switches running Native IOS. VACLs can be used in the following three ways:

1. Since the Catalyst SPAN capability is limited to LAN ports, how can a user analyze WAN links using the NAM-1/2? This can be done using one of two methods: VACLs and NetFlow Data Export feature, which is described shortly. The user can use a VACL to configure the WAN port data to be captured and forwarded to the NAM as Ethernet frames. This feature only works for IP traffic over the WAN interface
2. Secondly, VACLs can be used with LAN ports and is useful if no more SPAN sessions are available.
3. Also, VACLs can be used to help filter on specific types of traffic for further analysis by the NAM.

To configure VACLs, the user must use the CLI of the host switch. For further information on VACLs and their configuration, refer to the NAM User Guide and chapter 5 for links to references on VACL.

NAM-1/2 Data Sources

NetFlow



NAM Data Sources – NetFlow

Besides the NAM's internal interfaces for SPAN/VACL and mini-RMON, there is also one for NetFlow Data Export (NDE) packets arriving to the NAM via UDP port 3000 (management port –shared by NDE, ERSPAN, and management traffic). NDE packets contain information on one or more packet flows for one or more interfaces on a local or remote router that can be parsed and added to the RMON MIB and reported on by the NAM Traffic Analysis software. NetFlow allows for the monitoring of applications, hosts, conversations, and DiffServ (*remote*). *Detailed monitoring for voice, VLAN, ART, DiffServ (local) and packet captures and decodes are not available on NetFlow (NDE) data sources.*

The flows are configured on the remote device, possibly by interface, and exported to the NAM via UDP port 3000. The flows represent data coming in one interface on the remote device and exiting out another. If NDE is enabled on the host switch, all traffic that is layer 3 switched on the PFC and all traffic that is NetFlow switched on the MSFC are automatically forwarded to the NAM for potential monitoring.

For further information on NetFlow and its configuration, refer to the NAM User Guide and chapter 5 for links to references on NetFlow.

In general, it is extremely important to manage the data sources supplying data to the NAM. The user must understand how the NAM and its data sources are configured in order to help interpret the various NAM reports. Later in this chapter we will look at how to select and configure these data sources for monitoring by the NAM.

This page intentionally left blank.

CISCO SYSTEMS



Network Monitoring Using NAMs

NAM Hardware Overview

- Catalyst 6500 and 7600 Series NAM-1, NAM-2
- **Cisco Branch Routers Series NM-NAM**

Traffic Analyzer Software



Cisco Branch Routers Series NM-NAM Features

- **Multiple Sources for Analysis**
 - Internal Interface receives interface data streams via CEF
 - External Interface can be connected to FE LAN segment
 - NetFlow
- **Full RMON 2 Capability**
 - Hosts statistics –Network Layer
 - Conversation statistics –Network Layer
 - Upper layer protocol distribution
- **Extended RMON**
 - ART(Application Response Time)
 - DS-MON (Differentiated Services)
 - Voice over IP
- **MIB II support for hosting router interfaces**
- **NBAR-PD MIB**



NM-NAM Features

The Cisco® Branch Routers Series NAM, an integrated traffic-monitoring module for the Cisco 2600XM Modular Multi-Service Module, Cisco 2800 integrated services routers, Cisco 3660 Multi-Service Platform, Cisco 3700 Series Multi-Service Access Routers, Cisco 3800 Series integrated services routers, and the Cisco 2691 Multi-Service Platform routers, enables network managers to gain application-level visibility into network traffic.

The NM-NAM has two interfaces used for analyzing traffic. Router interface traffic can be forwarded to the Internal NM-NAM interface using Cisco Express Forwarding enabled from the router's CLI. The External interface can be connected to a Ethernet segment for analysis. Further, depending which port is designated as the management interface (receives NAM access traffic), that port can receive NetFlow traffic and analyze it as a separate data stream.

Note: The Traffic Analyzer does not have a mechanism for viewing the CEF configuration of each router interface. The user must have a prior information about the CEF configuration to properly understand the NAM analysis.

Included with the NAMs is an embedded, Web-based Traffic Analyzer, which provides full-scale remote monitoring and troubleshooting accessible through a Web browser. Analysis is done through the use of many different MIBs including RMON, ART (Application Response Time), DS-MON (Differentiated Services), and VoIP (Voice over IP).

The NM-NAM can also provide layer 2 statistics for each router interface by polling the router's MIB-II. Layer 3 statistics (apps, hosts, and conv) are also available for each interface by effectively creating a NetFlow for each enabled interface and forwarding it to the NAM. This processes is handled through the GUI via a simple enabling of the feature for desired interfaces. Alternatively, if NBAR is enabled, the NAM can use the NBAR-PD MIB to display application traffic seen on each interface of the router. This differs from the internal interface which presents an aggregate of this type of data for all interfaces forwarding packets.

Using the integrated NAM solution, Network Managers gain valuable insight into their networks with both real-time and historical application usage for performance monitoring and trending, fault isolation, and troubleshooting purposes.

NM-NAM Hardware Overview Specifications

	NM-NAM
SPECIFICATIONS <ul style="list-style-type: none">• Processor• Memory• Capture Buffer• Performance	500-MHz PIII 512MB 70 MB ~10- 45MBs
MONITORING APPLICATIONS	FE, T1/E1, ATM, T3, DSL
DEPLOYMENT SCENARIOS	BRANCH REMOTE OFFICES



NM-NAM Specifications

Hardware Architecture - Optimized performance single processor architecture with 256 MB of RAM and a 20 GB hard disk drive.

Monitoring Interfaces - Two Fast Ethernet monitoring interfaces: one "internal" backplane interface for receiving copy of LAN or WAN traffic sent through a special packet-monitoring feature in the router's Cisco IOS Software and one "external" interface for receiving traffic directly from local or remote LAN ports; either can be used for management traffic and for receiving NetFlow data (versions 1, 5, 6, 7, 8, and 9).

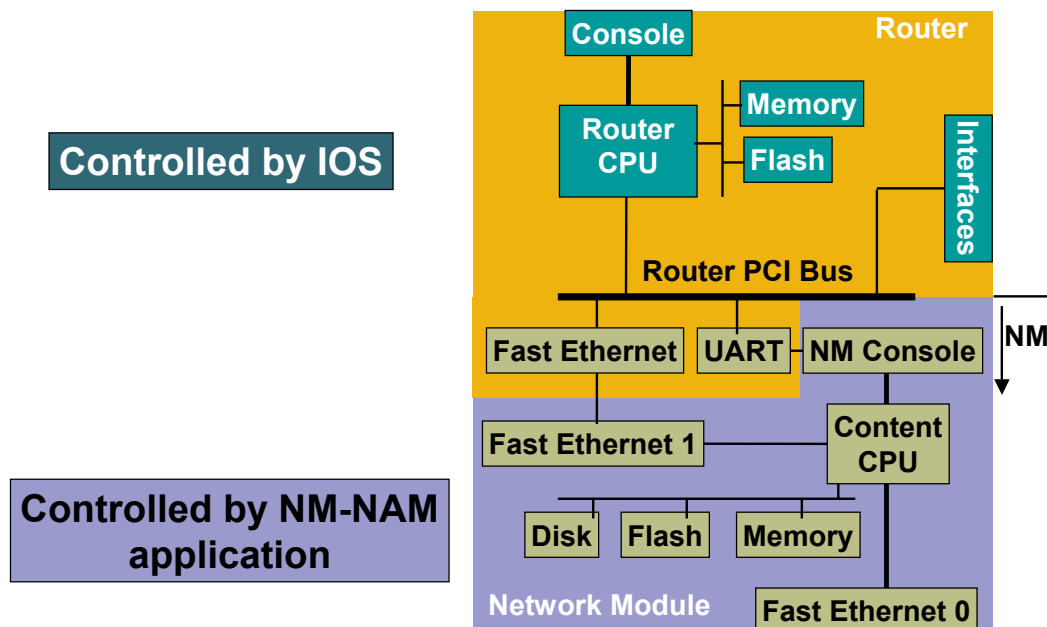
Performance - Fast Ethernet-class monitoring performance (while using internal monitoring interface; it is recommended to monitor up to 10 Mbps traffic on the Cisco 2600XM Series Modular Multi-Service Module, the Cisco 2691 Multi-Service Platform, and the Cisco 2800 Series integrated services routers, and up to 45 Mbps traffic on Cisco 3660 Multi-Service Platform, Cisco 3700 Series Multi-Service Access Routers, and Cisco 3800 Series integrated services routers; external monitoring interface can be used for higher-capacity monitoring).

Router Platforms - The Cisco Branch Routers Series NAM can be deployed in any network module slot in the Cisco 2600XM Series Modular Multi-Service Module, Cisco 2800 Series integrated services routers (except the Cisco 2801 Integrated Services Router), Cisco 3660 Series Multi-Service Platform, Cisco 3700 Series Multi-Service Access Routers, and Cisco 3800 Series integrated services routers. Only one NAM is supported per router chassis.

Cisco IOS Software- Cisco IOS Software Release 12.3(7)T or Cisco IOS Software Release 12.4(1) or later.

NM-NAM Hardware Overview

Architecture



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

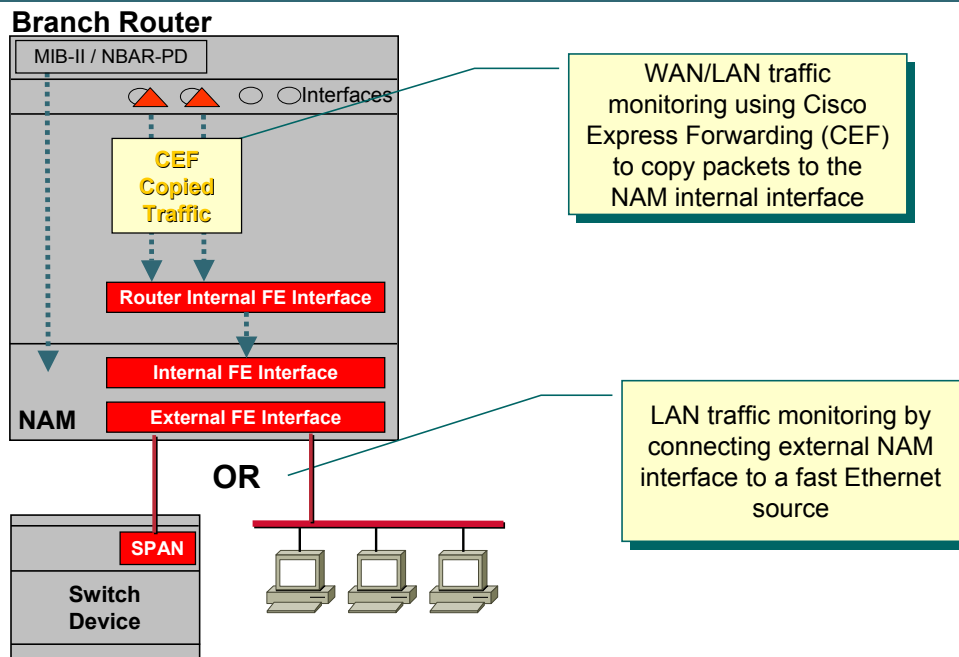
Product Features 2-20

NM-NAM Architecture

Data enters the NM-NAM for analysis via one of two interfaces on the NAM, the internal and external monitoring interfaces. One of these interfaces will also be used to receive all NAM access traffic (SNMP, HTTP, and telnet), as well as NDE traffic. The data, received in frame format, is parsed by the RMON process on the NAM and stored in the RMON, SMON, and other MIBs loaded onto the NAM. The polling process grabs data from these MIBs and performs the data analysis and presentation functions that generate the graphical tables and charts that you see. The analysis software responds to HTTP requests from a client's Web browser and presents the traffic reports and the configuration menus.

Note: Traffic forwarded to the Internal NAM monitoring interface is controlled by the host router.

NM-NAM Data Sources Interfaces



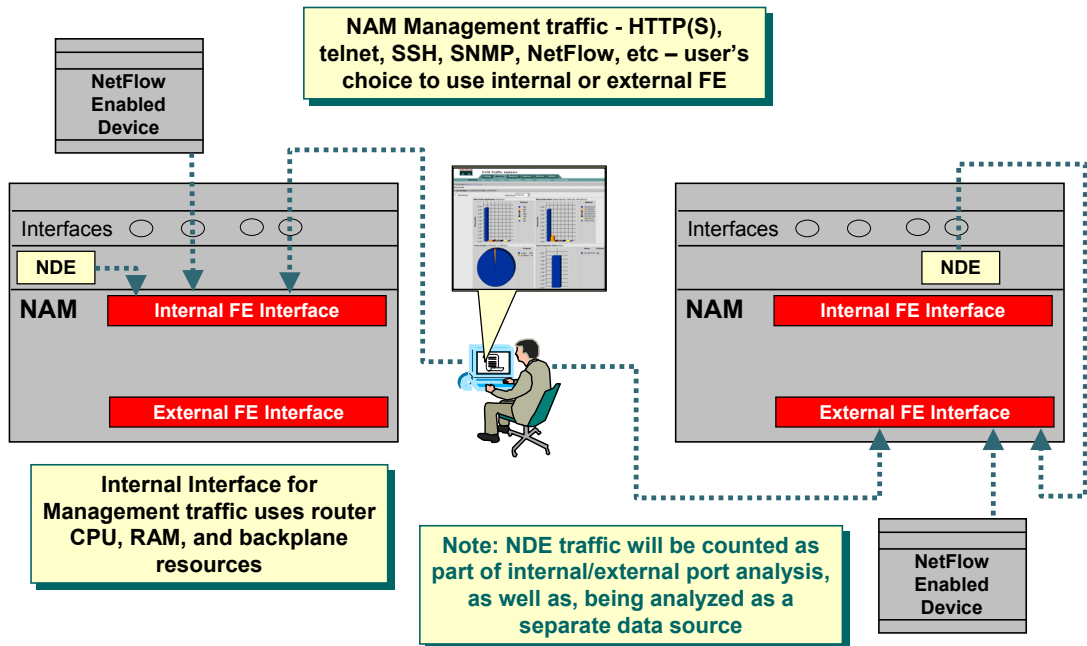
NM-NAM Data Sources - Interfaces

The NM-NAM allows for the direct monitoring and analysis of WAN interfaces by using CEF to copy the packets to the internal NAM interface for processing. When multiple interfaces are copied to the NAM, the NAM aggregates the data. CEF can be used to forward both WAN and LAN data streams.

The NM-NAM also has an external interface that can be used for monitoring and analysis of connected LAN links. This connection could be to a hub to view a LAN segment or to a Switch SPAN port for more flexible port and VLAN analysis.

NM-NAM Data Sources

NetFlow & Management Traffic



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-22

NM-NAM Data Sources – NetFlow and Management Traffic

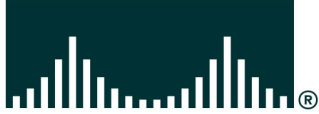
Besides presenting analysis of traffic flows seen by the internal and external interface, NetFlow data streams are also analyzed though they are received on either the internal or external interface. Since NetFlow traffic will be sent to the NAM on UDP port 3000, the analysis software is able to break it out as a separate data stream.

The interface used to receive the NetFlow data streams depend on which one of the NM_NAMs interfaces is configured to be in management mode. The interface configured to be in management mode will also be used to receive and send out the client http traffic, any SNMP requests of the NAM data, and any telnet session to the NAM itself. Obviously, if the internal interface is configured as the management interface (default) this will put additional stress on the router's resources. If the external interface is configured as the management interface, then it must be on a segment that allows access (i.e. not connected to a SPAN port on a switch).

Since the management traffic is received on one of the NAM ports, it will also be counted in the analysis of that interface.

In general, it is extremely important to manage the data sources supplying data to the NAM. The user must understand how the NAM and it's data sources are configured in order to help interpret the various NAM reports.

CISCO SYSTEMS



Network Monitoring Using NAMs

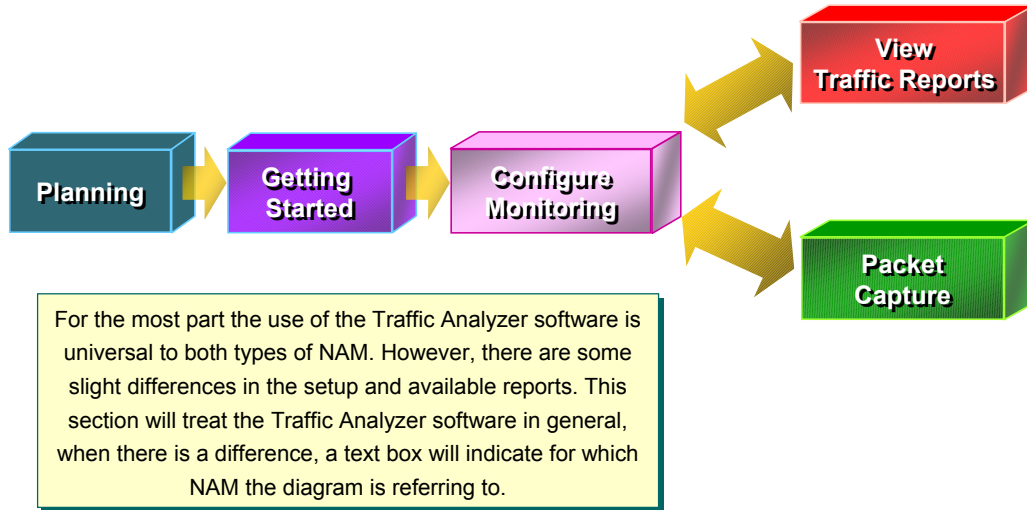
NAM Hardware Overview

Traffic Analyzer Software

- Planning
- Getting Started
- Configuring
- Viewing Reports
- Packet Capture and Decode



Road Map to Using NAMs

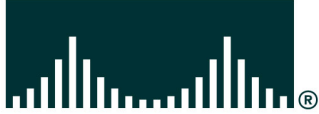


Network Analysis Module Road Map

The feature-rich architecture of the NAM enables you to gain different levels of visibility and perspectives on your network. You can use the NAM for acute problem resolution or for performance monitoring and network planning. You can view your network from an application response-time perspective, or from quality of service for voice and data. The wealth of possibilities for mining the NAM for valuable data means that you must identify what you want to use the NAM for and how to configure it to meet your needs. This road map is designed to do just that, to help you navigate the features and configuration options of the NAM to help you reach your destination. The next sections guide you through each of the steps illustrated in the figure above.

Note: For the most part the use of the Traffic Analysis Software is universal to both type of NAMs. However, there are some slight differences in the setup and available reports. This section will treat the Traffic Analysis Software in general. When there is a difference, a text box will indicate for which NAM the diagram is referring to.

CISCO SYSTEMS



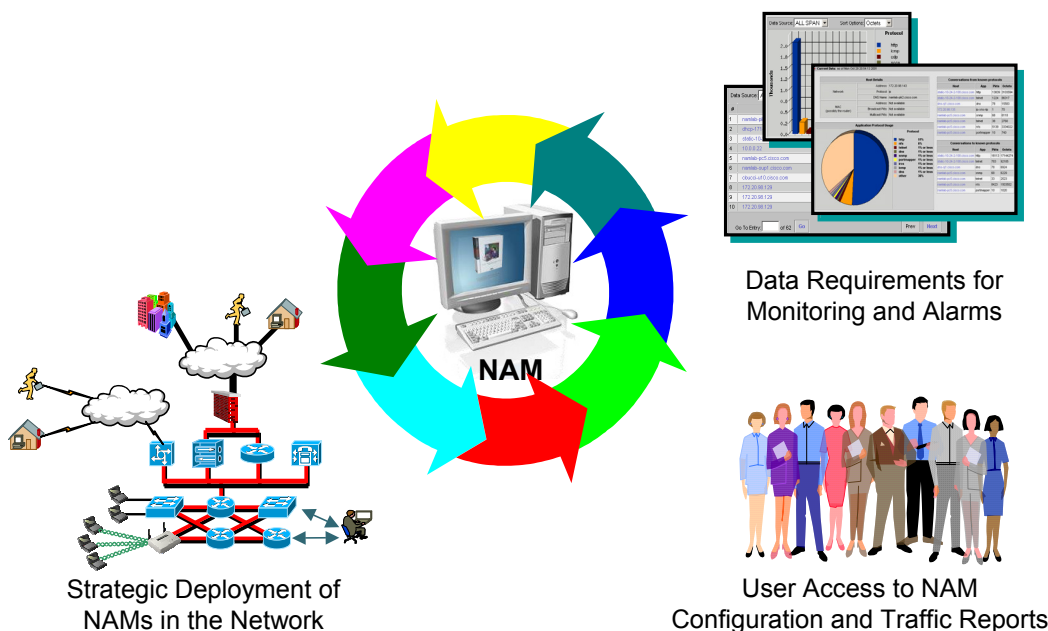
Network Monitoring Using NAMs

NAM Hardware Overview

Traffic Analyzer Software

- Planning
- Getting Started
- Configuring
- Viewing Reports
- **Packet Capture and Decode**





Planning for NAM Deployment

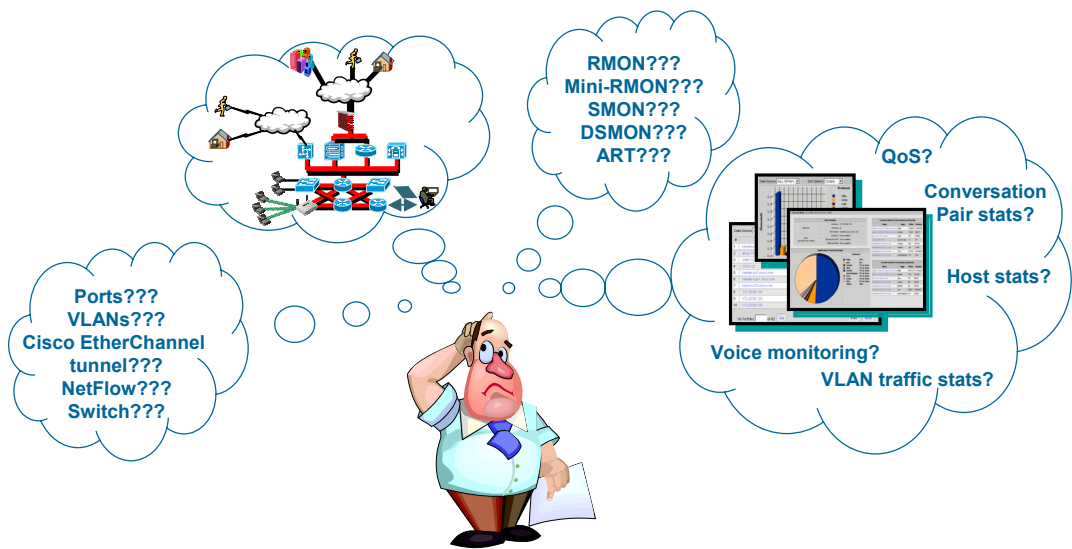
The data that the NAM collects, and the reports that it generates, will only be as good as the effort and consideration you put into the planning stages. You must bring your knowledge of your network and business, and how the business uses the network, into the planning stages when deploying the NAM to ensure that you collect the data you want, from the sources that make the most sense, and to present the data in the most productive way. Of course, the planning effort will vary according to your environment and objectives, but following are some variables that you should consider:

- What business or technical problem or problems are you trying to solve with the NAM?
 - A specific application or response-time problem?
 - Voice or data quality-of-service delivery?
 - Monitoring for real-time or historical performance?
 - Acute problems or fault isolation?
 - Some combination of these?
- How many NAMs and what types do you need, and where should you place them to accomplish your objectives?
- What data collection and monitoring/reporting functions will meet your objectives?
- What members of your organization can or will benefit by this data and reporting?

The upcoming pages discuss some of these issues, as do the scenarios in Chapter 3. Read on to find out how you can meet your monitoring needs with a thoughtful deployment of NAMs in your switched network.

Planning for NAM Deployment

Defining Data Sources and Reporting Requirements



Defining Data Sources and Reporting Requirements

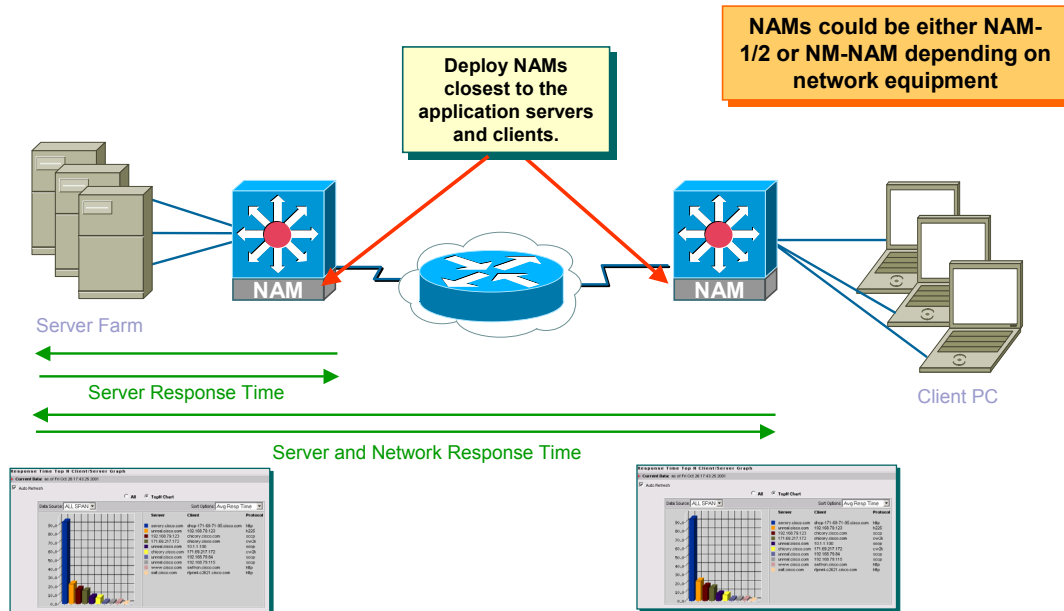
The NAMs are capable of receiving data from a number of sources for analysis by the Traffic Analyzer software, as such, data source selection requires careful consideration. The user must first determine what information is desired from the analysis software, and which data must be collected to get the desired reports. Properly determining the data to collect to meet end-users monitoring and reporting needs is perhaps the very crux of network management. The success of your NAM implementation depends on a clear understanding of these end-users needs and how to provide the data via the NAM. To gain a better understanding of this issue, consider the following questions:

- What data does the NAM collect?
- Where can it collect data from, and does NAM placement affect the data collection?
- What reporting does the NAM offer?

These planning and deployment issues are covered in this chapter, and the scenarios in Chapter 3 illustrate how to deploy, configure, and use the NAM to solve real-world problems. First, however, we discuss what the NAM collects and where it collects it from. This discussion will help you answer the questions posed above.

Planning for NAM Deployment

Application Response-Time Problems



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-28

Deployment for Application Response Time Problems

One true validation of the performance of a network is how well the applications run over the network, because this variable most closely represents the user's experience of the network. So, measuring critical application response times is one effective barometer of the performance of your network. The NAM, using the ART MIB, does this by capturing packets, time stamping them, and measuring the time between a client request and the fulfillment of that request by the server. This information helps you identify where the application delays are occurring—at the server, on the network between the client and server switch, or at the client.

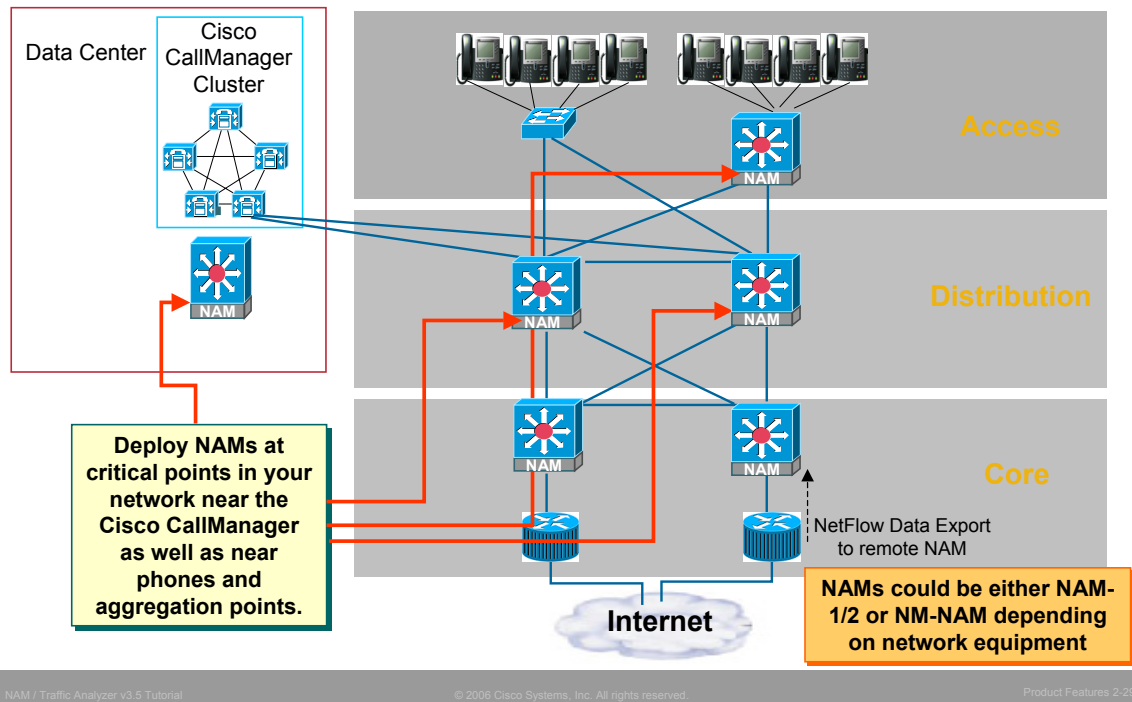
For response-time monitoring, it is very important to identify what response times you really want to measure so you can gather the most accurate data and reports. For example, if you want to gather statistics about how long it takes the server to complete a request (server think time), place a NAM close to the server. If you want to gather information about both server think time and the time it takes the network to transmit the data (flight time), then place the NAM closest to a client that uses the application on the server. We cannot stress enough how critical NAM placement is for response-time reporting: the more accurate your understanding of how the NAM collects these statistics and hence your accurate placement of the NAM, the more meaningful your response-time data will be.

In addition to response-time reporting, you can also use other reporting features such as application statistics, TopN talkers to the server, conversations between the server and clients to identify who the server is talking to and what its bandwidth consumption is for each pair, or utilization or errors on the switch port that the server connects to. All these perspectives and options help you both identify trends in the performance of the application server and troubleshoot problems when they arise.

For acute application or network performance problems, you can use the NAM packet decode feature to view traffic on a packet-by-packet basis.

Planning for NAM Deployment

Voice Monitoring



Deployment for VoIP problems

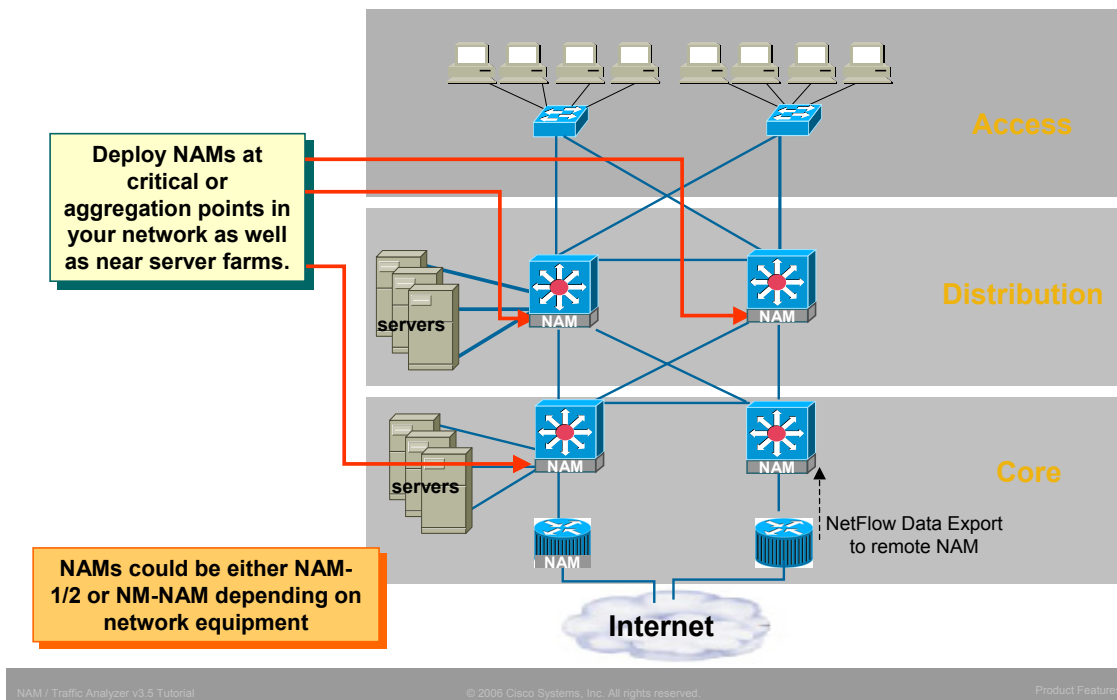
Performance monitoring of voice applications is critical because voice traffic is much more sensitive to certain fluctuations in network performance than data. For example, voice traffic cannot tolerate variable delays in the delivery of packets in the same way that data can. Users, who've come to expect the high quality of voice transmission, will be able to discern this variation in delay, known as jitter. Proactively monitoring voice applications will enable you to deliver high-quality voice services before users experience any degradation. After you isolate the source or location of the delay, you can then implement quality-of-service (QoS) policies to ensure better performance.

To monitor voice traffic, NAMs should be deployed at various points in the network: in switches at the access layer that connect users with IP phones to the network; in distribution layer switches that connect access layer switches to the Cisco Call Manager, and perhaps in routers at branch offices. Perhaps the most useful placement of a NAM for voice monitoring is near the Cisco CallManager Cluster. Monitoring network access to the Cisco CallManager will provide a rich source of information about the performance of the voice system. This instrumentation strategy will help you identify performance problems such as jitter and packet loss for all IP calls.

Other NAM features can also be used to gather statistics on voice applications. RMON can be used to collect protocol statistics on protocols such as Skinny Call Control Protocol (SCCP), H323, Media Gateway Control Protocol (MGCP), and Session Initiation Protocol (SIP). You can also gather response-time statistics on voice applications. Again, alarms can be defined to notify you when voice packet loss or jitter signals the degradation of voice application performance. In addition, you can configure the NAM to provide reports on users and call statistics for troubleshooting or other purposes.

Planning for NAM Deployment

Performance Monitoring



Deployment for Performance Monitoring

As mentioned earlier, the NAM offers network managers a wealth of data because of the MIBs that the NAM supports. You can collect utilization, error, Media Access Control (NAM-1/2 only), network and application layer host and conversation statistics in real time. You can also extend monitoring by creating thresholds for data stored in the MIBs to notify you when performance on your network degrades. So, in addition, to having a passive monitor that provides you visibility about network performance, you can configure the NAM to proactively notify you when conditions change.

The NAM also provides the ability to determine trends of your network performance over time (historical reporting) for a 100 day interval (data source must remain fixed for reporting duration).

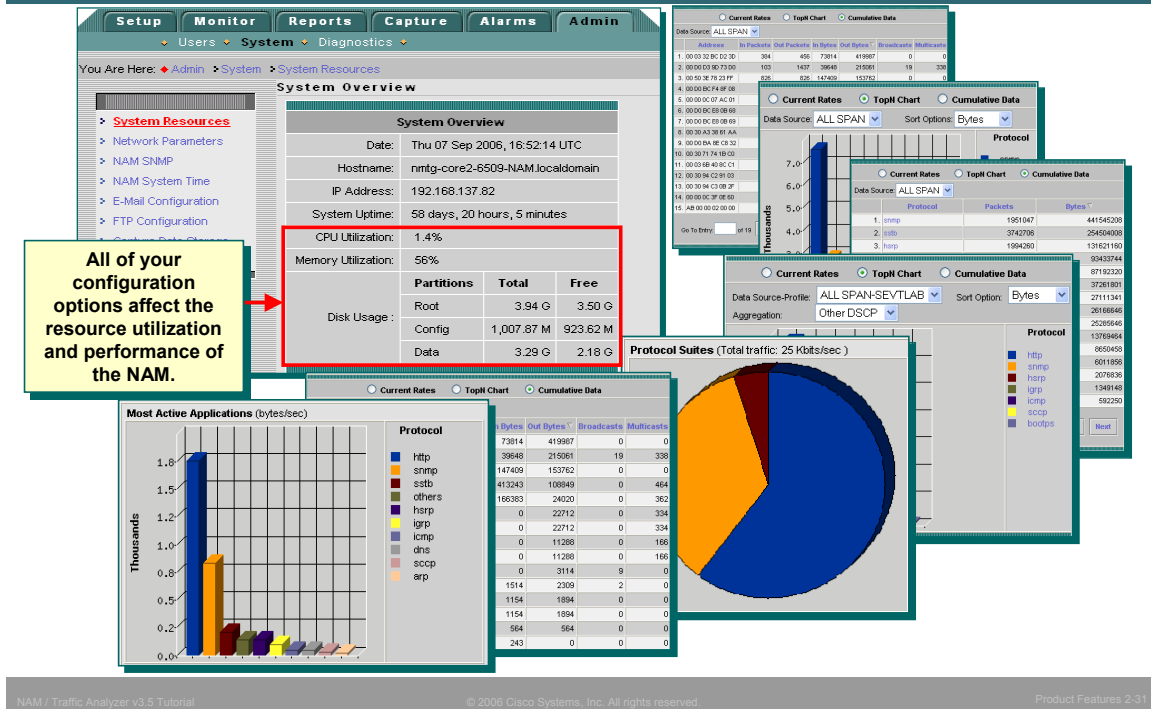
You can also use the NAM alarm features to notify you when conditions on your network fall below your expectations. For example, you could set alarms using thresholds for port utilization, broadcast traffic, errors, or host or conversation pair traffic volumes.

To use the NAM for real-time monitoring of your network and determining trends over time, NAMs should be deployed in server farms located in the distribution and core layers. You may also consider deploying NAMs at LAN aggregation points, or in routers that provide building-to-building connectivity. Consider spanning trunk ports for resource usage and distribution patterns of potential network bottlenecks. You can also gather layer 2 statistics for every port on the switch (NAM-1/2) or interface (NM-NAM) without impacting the NAM performance because these statistics are pulled directly from MIBs on the NAM host.

With different hardware versions of the NAM available, deployment choices can be based on both performance and economic requirements. The NAM-2 has higher monitoring capacity, as well as two data ports for Spanning and VACLs, and is best suited for deployment in large core or distribution layer switches with highly used gigabit links. The NAM-1 is a more effective and economical solution at branch offices, smaller core, distribution, and access layer switches. The NM-NAM allows for direct WAN monitoring in branch routers and can also be used to monitor LAN links as well.

Planning for NAM Deployment

NAM Performance Considerations



NAM Performance Considerations

The NAM offers a wealth of data and reports that give you visibility into your network. The next section shows you how to choose from among the data sources available to you and how to tailor the NAM monitoring and reporting functions to meet your specific needs. While we go through the setup section and, more importantly, while you develop your NAM usage plan, keep in mind that the NAM has fixed resources and all of the monitoring reports, alarms, and captures you define are stored in the NAM memory (which is currently 512 MB for the NAM-1 and NM-NAM, and 1 GB for the NAM-2). So all of the ways the NAM delineates data for the monitoring and reporting you choose, and all of the packets you capture for decode will consume memory.

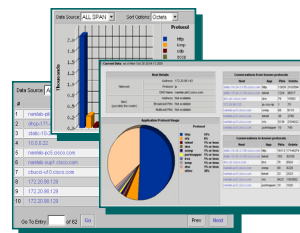
Be aware that the more traffic you collect, the more NAM resource you are consuming. So, choose your data sources and your monitoring and reporting needs wisely to ensure that you maintain the validity of your data. A good practice is to slowly and incrementally add data collection and monitoring options and then view their impact on the NAM by viewing system resource utilization in the [Admin > System > System Resources](#) menu.

Planning for NAM Deployment

Users, Security, and NAM Access

Users	Account Mgmt	System Config	Capture	Alarm Config	Collection Config	Collection View
<input type="radio"/> admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a user then take an action-->						
Create Edit Delete						

Which users should have access to which features?



Define security policies to protect your data requirements.



Define security policies that meet your security needs and NAM users' functional requirements.











Enable third-party management systems to communicate with the NAM via SNMP community strings.

Users, Security, and NAM Access Considerations

Network management systems are a funny thing when it comes to security and access. You may need to define different levels of security to meet your users' varying needs. In-depth configuration and customization of the NAM to deliver the monitoring needed requires a certain level of access. Whereas monitoring and reporting features of the NAM often serve a broad range of users who have different security requirements. These issues may be true of the NAM in your environment because you may want to give many users access to some parts of the NAM and secure other parts. However, giving unlimited access to all the NAM features could undermine the very purpose for deploying NAMs in the first place. The problem is this: As discussed earlier, the data you get from the NAM is only as good as your planning for and configuration of it. So, if you give configuration access to all your users, you will not be able to guarantee that the collections you configured a week ago will still be the same when you go to review the performance of your network. For example, let's say you have configured the NAM for alarming and event notification on a data source for historical reporting. Any changes made to the NAM may disable the alarms you rely on for notification or the data sources you are using for monitoring. So, when planning for the NAM deployment, consider who should have access to its configuration utilities and who simply needs access to the reports. Doing so will help ensure that the NAM will continue to deliver the data you need.

Planning for NAM Deployment

Summary

-  Identify the problems or needs you are trying to solve with the NAM.
-  Identify what data collection and monitoring needs will help resolve problems or needs.
-  Determine how many NAMs you will need to deploy and where you need to deploy them.
-  Identify the appropriate SPAN sources – port, VLAN, or Cisco EtherChannel tunnel for each NAM.
-  Define access policies, data collection and reporting, and alarm configuration requirements for each NAM to match needs.
-  Configure security, monitoring, and alarming as defined in the previous steps.
-  Review NAM system resources to ensure that NAM will continue to support your collection and monitoring needs.
-  View, modify, and monitor the configuration as necessary.

Planning Summary

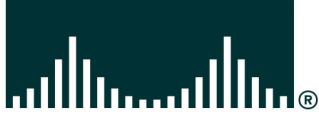
Obviously, there is no easy formula for determining how many NAMs you will need, where the NAMs should be deployed, and how they should be configured. It depends on what business or technical problems you are trying solve. And those are just some of the things you need to consider. In short, following are some guidelines for planning and implementing the NAM:

- Identify the problem or need you want to resolve with the NAM.
- Identify what data and reports will help resolve the problems or needs.
- Determine how many NAMs you need and where you need to deploy them.
- Identify the appropriate Data sources—port/interface, segment, VLAN, or Cisco EtherChannel® tunnel—for each NAM.
- Define what access policies, data collection and reporting, or alarm features are needed for each NAM.
- Configure security, monitoring, and alarms to meet the needs defined previously.
- Review NAM system resources to ensure that NAM resources remain low enough to support your data collection and monitoring needs.
- View and modify your reports and configuration as necessary.

We have identified some strategies and considerations for the first three steps. The next section covers how to configure access, data sources, data collection and reports, and alarms to deliver the monitoring you need.

This page intentionally left blank.

CISCO SYSTEMS



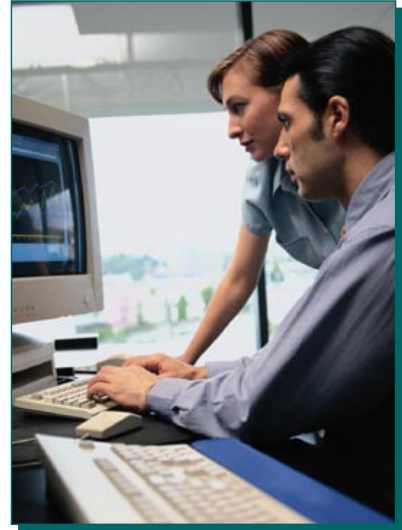
Network Monitoring Using NAMs
NAM Hardware Overview

Traffic Analyzer Software

- Planning
- **Getting Started**
- Configuring
- Viewing Reports
- Packet Capture and Decode



- **NAM Hardware Installation**
- **NAM User Interface**
- **NAM Network Configuration**
- **Securing Access to the NAM**
 - Creating New Users
 - TACACS+
 - SNMP Communication
- **Viewing Access Logs**
- **Setting NAM System Time**



Getting Started

Getting started with the NAM is a straightforward process, made easier by the fact that the NAM is an integrated management system on a card. As you will see shortly, once the module is installed, you will simply need to configure its network parameters and additional user accounts, if needed. This section will also discuss various security mechanisms available for using TACACS+ and access to the NAM using SNMP, instead of accessing the web server using HTTP. So let's get started!

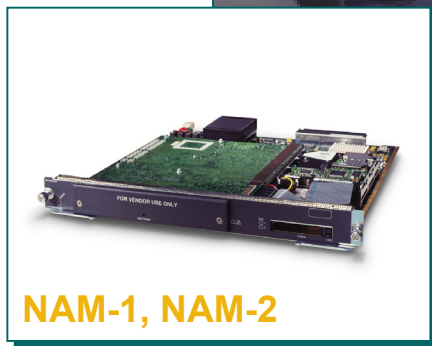
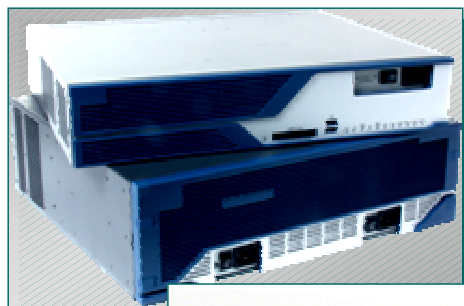
Getting Started

NAM Hardware Installation Overview

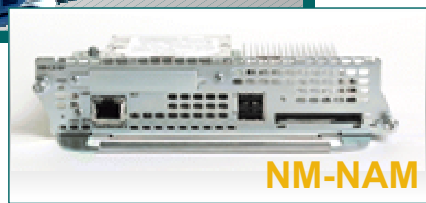
Cisco Catalyst 6500 Series or Cisco 7600 Series



Cisco ISR 2600XM, 2800, 3660, 3700, 3800, 2691 Series Routers



NAM with Integrated Traffic Analyzer Software



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-37

NAM Hardware Installation Overview

NAM-1 and NAM-2

The NAM-1/2 installs into a single slot on the Cisco Catalyst® 6500 series and Cisco 7600 series chassis. The host switch must meet the required operating system (OS) versions. A complete listing of supported OS and supervisor hardware can be found in Chapter 4. The NAM can be installed in any slot on the host Cisco Catalyst® Switch, except for the slot(s) that are reserved for the Supervisor module(s). After the NAM is installed, check that the NAM status is OK by using the `show mod command` via either CatOS or IOS.

NM-NAM

The NM-NAM installs into a single slot on the Cisco 2600XM, 2800, 3660, 3700, and 3800 Series access routers. The host router must meet the required operating system versions. A complete listing of supported OS and hardware can be found in Chapter 4. After you have installed the NAM into the chassis, check that the status of the enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

Note(s):

- Refer to Chapter 4 in this tutorial for more detailed guidelines on installing and troubleshooting the NAM and the appropriate NAM Installation Guide for more detailed instructions on configuring these parameters.

Getting Started

NAM User Interface – Traffic Analyzer

The image shows two screenshots of the NAM Traffic Analyzer web interface. The top screenshot is the login page, and the bottom screenshot is the System Overview page. A red arrow points from the login page to the System Overview page, indicating the transition after a successful login.

Login Page:

- Address bar: `http://192.168.159.118/auth/login.php`
- Page Title: **NAM Traffic Analyzer**
- Form Fields:
 - Name: `admin`
 - Password: `*****`
- Buttons: `Login`

System Overview Page:

- Page Title: **NAM Traffic Analyzer**
- Navigation Tabs: `Setup`, `Monitor`, `Reports`, `Capture`, `Alarms`, `Admin`
- System Overview Table:

System Overview			
Date:	Thu 07 Sep 2006, 16:52:14 UTC		
Hostname:	nmtg-core2-6509-NAM.localdomain		
IP Address:	192.168.137.82		
System Uptime:	58 days, 20 hours, 5 minutes		
CPU Utilization:	1.4%		
Memory Utilization:	56%		
Disk Usage:	Partitions	Total	Free
	Root	3.94 G	3.50 G
	Config	1,007.87 M	923.62 M
	Data	3.29 G	2.18 G

NAM User Interface – Traffic Analyzer

Once you have enabled the HTTP web interface on the NAM (see Chapter 4 for details), you can begin using the embedded Traffic Analyzer software to both configure the NAM and view its traffic reports.

To access the NAM via HTTP, simply enter the IP address of the NAM (or Domain Name System [DNS] name) that was assigned during installation in the address field of your web browser. This brings you to the NAM login screen as shown in the illustration above. Enter the default username and password that was defined when the web interface was enabled. After entering the username and password, press the *Login* button. The opening web page for the NAM's Traffic Analyzer, the System Overview screen, will appear if your account information is authenticated.

Getting Started

Traffic Analyzer - Menu Options

The screenshot shows the NAM Traffic Analyzer web interface. At the top, there are six tabs: Setup, Monitor, Reports, Capture, Alarms, and Admin. Below the tabs is a navigation bar with links for Users, System, and Diagnostics. The main content area is titled 'System Overview' and contains a table of system statistics and a list of submenus on the left.

Callout boxes provide the following information:

- Options for configuring the NAM data collection and report functions.** (Points to the Setup tab)
- Options for viewing data.** (Points to the Monitor tab)
- Options for configuring & viewing historical reports** (Points to the Reports tab)
- Packet Capture and Decode Options** (Points to the Capture tab)
- Viewing Alarms Generated by the NAM** (Points to the Alarms tab)
- NAM Administrative Functions** (Points to the Admin tab)
- Available Options for the Selected Tab** (Points to the System submenu)
- Navigation bar shows you where you are within the NAM menu options.** (Points to the navigation bar)
- Available Submenus for Selected Function Option** (Points to the System submenu)
- Content window** (Points to the System Overview content area)

The 'System Overview' table shows the following data:

System Overview			
Date:	Thu 07 Sep 2006, 16:52:14 UTC		
Hostname:	nmtg-core2-6509-NAM.localdomain		
IP Address:	192.168.137.82		
System Uptime:	58 days, 20 hours, 5 minutes		
CPU Utilization:	1.4%		
Memory Utilization:	56%		
Disk Usage :	Partitions	Total	Free
	Root	3.94 G	3.50 G
	Config	1,007.87 M	923.62 M
	Data	3.29 G	2.18 G

The left sidebar shows the following submenus for the 'System' tab:

- System Resources
- Network Parameters
- NAM SNMP
- NAM System Time
- E-Mail Configuration
- FTP Configuration
- Capture Data Storage
- Web Publication

Traffic Analyzer – Menu Options

Everything you need to configure and use the NAM is available to you via the six tabs in the upper portion of the screen. Following is a brief description of each of the functions found under the tabs.

Setup Tab: Options for configuring the NAM for data sources, monitor views, protocols collected, alarms, and customization of graphs, charts and tables

Monitor Tab: Support for tasks that enable you to monitor the NAM such as the tables and graphs that you configured during setup

Reports Tab: Tools to configure and view historical reports about various traffic statistics

Capture Tab: Options to set up, start, stop, and decode the packet analysis functions

Alarms Tab: Options to view alarms generated by the NAM that were configured during setup

Admin Tab: Options for setting up and configuring the administrative tasks such as user management, security, SNMP parameters, NAM network parameters

After selecting one of the major function tabs, the options associated with the tab appear below the tabs. Selecting one of these options may or may not have associated sub-tasks and will be displayed on the left side of the NAM Traffic Analyzer window. At any time, the current context (path to the displayed task) is displayed on the "You Are Here" context line. Clicking on any layer of the context line will take you back to the associated display.

Let's look at each of the options under these tabs.

Getting Started

Navigation Menu

Setup	Monitor	Reports	Capture	Alarms	Admin
Configure All Monitoring Options	View All Data Collection Reports	Configure and View Historical Reports	Set and Run Packet Capture Options	View All Alarm Reports	Configure NAM Options
Switch/Router Parameters: Setup NAM communication with host device	View Overview of several statistics	Basic: Reports for application, host, conversation, voice, DiffServ, and ART	Buffers: Set up and manage capture buffers (including capture filters). Start and stop capture. View and decode captured packets.	NAM: View alarms generated by NAM (applications, conversations, hosts, voice, ART, DiffServ)	User: Configure Web users and TACACS+
Data Source: Configure SPAN and NetFlow sources	View Application Statistics	Custom: Combine multiple basic reports into single custom report	Files: Save packets in capture buffers to files. Decode and download files.	Switch: View Port Level Alarms (6k-NAM only)	System: View system resources, and configure NAM parameters
Monitoring: configure data collection	View Voice Statistics	Scheduled Export via Email or FTP	Configure custom filter options		Diagnostics
Protocol Directory: Setup application protocols	View Host Statistics				
Alarms: Configure alarm parameters	View Conversation Statistics				
Preferences: Configure interface preferences	View VLAN Statistics (6K-NAM only)				
	View DiffServ Statistics				
	View Application Response Time Statistics				
	View Device Based Statistics				
	View MPLS Stats (6K NAM only)				

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-40

Navigation Menu

The user interface for the NAM Traffic Analyzer has six tabs in the upper third of every window. You will find all the options you need to configure the NAM monitoring and to view reports based on collected data under these six tabs. The figure outlines the configuration or viewing options available under each tab. It is useful to remember that the data that can be viewed under the Monitor tab is the result of the configuration options you selected and executed under the Setup tab. In other words, if you do not see the data or reports you want under the Monitor tab, return to the Setup tab to verify that you configured the NAM correctly.

Similarly, alarms generated by the NAM can be viewed under the Alarms tab. Remember, however, that the alarms you view under the Alarms tab are generated based on the configuration options you selected under the Setup tab. You do have a few options for configuring how the data is presented to you within the Monitor and Alarms tabs, but keep in mind that these options enable you to manipulate only the data that has already been configured for collection under the Setup tab. So, if you do not see the data you expect to see, or if you just want to validate the data you do see, review the configuration options you made under the Setup tab.

Getting Started

NAM Network Configuration

CISCO SYSTEMS

NAM Traffic Analyzer

Help | Logout | About |

1 Admin

2 System

3 Network Parameters

You Are Here: Admin > System > Network Parameters

Network Parameters

Network Parameters	
IP Address:	192.168.137.82
IP Broadcast:	192.168.137.83
Subnet Mask:	255.255.255.252
IP Gateway:	192.168.137.81
Host Name:	nmtg-core2-6509-NAM
Domain Name:	localdomain
Nameservers:	171.70.168.183
	171.68.226.120

Apply Reset

Instructions

Use this screen to configure the NAM network parameters.

NOTE: Network connectivity may be lost, if an invalid or incorrect IP address or gateway is set.

Network access configuration options that were defined during installation at the command-line interface can be modified in this submenu

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-41

NAM Network Configuration - Configuring the NAM for Access

When the NAM is physically in the chassis, you need to configure the NAM to provide it with network parameters to enable it to communicate. These parameters include standard network addresses, such as IP address and host name, default gateway, and domain name.

Before you can access the NAM across the network, the initial setup of these network parameters are configured via the command-line interface (CLI) of the NAM, discussed in Chapter 4. After you have set these parameters, you can then change them via the Web interface, as shown above. The figure shows the network parameters that can be changed on the NAM, such as: IP address, IP broadcast, subnet mask, gateway, host name, domain name, and name servers.

Getting Started

Securing Access to the NAM

TACACS+ Password Authentication

☐ Enable TACACS+ Authentication and Authorization

Primary TACACS+ Server:

Backup TACACS+ Server:

Secret Key:

Verify Secret Key:

User Account Management

	Users	Account Mgmt	System Config	Capture	Alarm Config	Collection Config	Collection View
<input type="radio"/>	admin	✓	✓	✓	✓	✓	✓
Select a user then take an action -->					<input type="button" value="Create"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

SNMP Parameters

System Group

Description: Cisco Network Analysis Module (WS-SVC-NAM-2), Version 3.5(1)
Compiled 2006.06.12 14:51:24 by pwildt Copyright (c) 1999-2006 by cisco Systems, Inc.

Uptime: 58 days, 20 hours, 24 minutes

Contact:

Name:

Location:

NAM Community Strings

<input type="radio"/>	*****	read-write
<input type="radio"/>	*****	read-only

Select an item then take an action -->

NAM Access Control

Audit Trail

Time ▼	User	From	
07 Sep 2006, 16:52:13	admin	10.21.89.164	User login
07 Sep 2006, 15:06:21	admin	10.70.230.54	User login
07 Sep 2006, 14:33:27	admin	144.254.200.222	User login
07 Sep 2006, 07:34:57	admin	64.104.5.212	Report created: Top-Apprication
07 Sep 2006, 07:19:37	admin	64.104.5.212	Report created: NAM_Training
07 Sep 2006, 07:18:53	admin	64.104.5.212	Report created: TOS ToS1 3GPP2-A10
07 Sep 2006, 07:17:30	admin	64.104.5.212	User login
07 Sep 2006, 07:17:23	admin	64.104.5.212	Access denied (no login session) /report/config.php

Securing Access to the NAM

As mentioned in the planning discussions earlier, you should consider carefully how you want to secure the NAM because any configuration changes made to the NAM may affect the monitoring you rely on for reporting, notification, and decision making. With the NAM, you have several levels of security you can use to define access to the NAM.

- You can create users with different levels of access on a per-user basis.
- TACACS+: You can configure the NAM to use a TACACS+ server to authenticate and authorize user access to the NAM.
- Define SNMP community strings to enable SNMP management systems to have read or write access to the NAM.

Configuration options for each of these are covered in the next few pages.

Getting Started

Creating New Users

The screenshot shows the NAM Traffic Analyzer web interface. At the top, there's a navigation bar with tabs: Setup, Monitor, Reports, Capture, Alarms, and Admin (circled with a red circle and labeled '1'). Below the navigation bar, there's a sidebar with a tree view showing 'Users' (circled with a red circle and labeled '2') and 'Local Database' (circled with a red circle and labeled '3'). The main content area displays a table of existing users and their privileges. Below the table are buttons for 'Create', 'Edit', and 'Delete'. A 'New User' popup box is shown on the right, with fields for Name, Password, and Verify Password, and checkboxes for various privileges.

Users	Account Mgmt	System Config	Capture	Alarm Config	Collection Config	Collection View
<input type="radio"/> admin	✓	✓	✓	✓	✓	✓
<input type="radio"/> guest	✓	✓	✓	✓	✓	✓
<input type="radio"/> Rada			✓			✓

Click **Create** to add a new user. Use the New User popup box to configure the user's password and privileges.

This table displays existing user accounts and access privileges.

New User

Name: Bob

Password: ••••••

Verify Password: ••••••

Privileges:

- ☐ Account Mgmt
- ☐ System Config
- ☒ Capture
- ☒ Alarm Config
- ☐ Collection Config
- ☒ Collection View

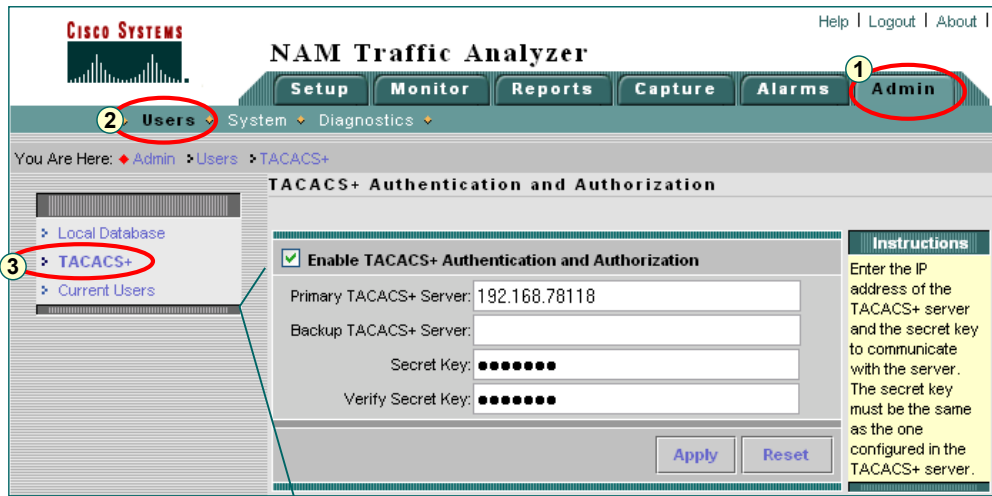
Submit Reset

Creating New Users

The NAM enables you to add various levels of security to user accounts. The first level of security is assigning passwords to user accounts. The second level of security is to configure user accounts to limit access based on the NAM feature set. Privileges associated with NAM features include: account management, system configuration, packet capture and decode, alarm configuration, collection configuration, and viewing. These configuration options enable you to limit access to the NAM based on a user's functional needs. For example, engineers responsible for fault management systems can be given access to collection and alarm configuration to define alarms and notification. Engineers responsible for troubleshooting may be given collection view and capture access privileges. Network planners may be given collection configuration and view access privileges. You may want to consider assigning all access to one person responsible for overseeing the various needs of users in your organization. It is up to you to decide which users need access to each of the features available. All users by default have the "Collection View" user privilege allowing all users to view any report for the collected data.

Getting Started

Using TACACS+ for Authentication



Enable TACACS+ services by clicking on the Enable box and entering the TACACS+ server IP address and key parameters that you configured on your TACACS+ server for the NAM.

Configuration instructions are provided in a box to the right of many configuration screens.

Using TACACS+ for User Authentication

On the previous page, we created users and assigned passwords to each user. The NAM also supports additional password security by adding TACACS+ server support for authenticating users configured for NAM use. TACACS is an authentication protocol that provides remote access authentication, authorization, and related services. With TACACS, user passwords and privileges are administered in a central database to provide scalability. To use TACACS+ services with the NAM, you must first have or install a TACACS+ server and configure the TACACS+ to include an account for the NAM. TACACS+ user groups should be created for each privilege type. NAM privileges are configured in the TACACS+ server as IOS Shell commands (refer to the NAM User Guide for more information on the NAM TACACS+ configuration options for NAM privileges). Refer to your individual TACACS+ installation and user guides for instructions on configuring your TACACS+ server.

When you have completed the TACACS+ server configuration, simply use the **Admin > Users > TACACS+** task to enter the IP address of the TACACS+ server and the keys you assigned for the NAM on the TACACS+ server to complete authentication services between the NAM and the TACACS+ server.

Getting Started

Third Party NMS Access to NAM using SNMP

Configure NAM community strings to allow 3rd party NMS to retrieve MIB information from NAM using SNMP; **SNMP v1/v2** supported.

Disable SNMP communication by deleting SNMP community strings

Choose **Create** to add community strings, or to delete, click the radio button to the left of the string to delete and click **Delete**.

The screenshot shows the NAM Traffic Analyzer web interface. At the top, there is a navigation bar with tabs: Setup, Monitor, Reports, Capture, Alarms, and Admin. The Admin tab is selected and circled with a red circle and the number 1. Below the navigation bar, there is a sidebar menu with options: Users, System, and Diagnostics. The Users option is circled with a red circle and the number 2. The System option is selected, and the Diagnostics option is expanded, showing a list of sub-options: System Resources, Network Parameters, NAM SNMP, NAM System Time, E-Mail Configuration, FTP Configuration, Capture Data Storage, and Web Publication. The NAM SNMP option is circled with a red circle and the number 3. The main content area displays the 'System SNMP' configuration page. It includes a 'System Group' section with fields for Description, Uptime, Contact, Name, and Location. Below this is the 'NAM Community Strings' section, which has two radio buttons for 'read-write' and 'read-only' community strings. At the bottom of this section are 'Create' and 'Delete' buttons. A text box on the right side of the screenshot explains that configuring Contact, NAM name, and NAM location are optional parameters but facilitate the use of the NAM for engineers who may be using it with other third-party network management systems as well as existing NAM users.

Third Party SNMP NAM Access

The last security configuration option available on the NAM is for configuring community strings. An SNMP community is a domain of one or more SNMP agents and one or more SNMP management consoles that share access information and configuration. Communities are formed by configuring each member of the community with a “string” (either read-only or read-write in this case) to indicate its membership in the community. In other words, community strings are similar to passwords, and they enable network management agents and consoles to agree on what information and configuration options can be shared. For example, if a network management console wants to retrieve information from an agent, the console must be configured with the read-only “community string” of that agent to read data from it. If it wants to also set parameters on the agent, it must be configured with the read-write community string.

When you configure your NAM community strings in the menu illustrated above, you are configuring community strings that another third-party, external management console must use to collect information from or send information to the NAM. To do so, simply click on the *Create* button and add the community strings for read-only and read-write. To prevent any outside SNMP access to the NAM, simply do not configure the SNMP strings.

Getting Started

Host Device Parameters - SNMP

Setup > Switch Parameters > Switch Information

Switch Information	
Performing SNMP test from NAM (192.168.159.118) to switch (192.168.159.117)	
Name:	nmtg-hq-core-6506
Hardware:	Cisco Systems Catalyst 6500 6-slot Chassis
Supervisor Software Version:	IOS Version 12.2(14)SX1
System Uptime:	12 days, 5 hours, 10 minutes
Location:	N/A
Contact:	N/A
SNMP read from switch:	OK
SNMP write to switch:	OK
Mini-RMON on switch:	Available
NBAR on switch:	Unavailable
VLAN Traffic Statistics on supervisor:	Available
NetFlow Status:	Configured to NAM 172.20.111.163 on port 9991

Information about the host switch and available data sources (VLAN, NetFlow, NBAR)

NAM-1 and NAM-2

Enter the same IP address and read-write community string as was configured on the router. Otherwise the NAM cannot communicate via SNMP with the router

NM-NAM

Setup > Router Parameters > Router Information

Router System Information	
Name:	nmtg-hq-core-3725
Hardware:	3725 chassis, Hw Serial#: JMX0709L4QR, Hw Revision: 0.1
Router Software Version:	Version 12.3(4)XD2
Router System Uptime:	12 days, 0 hours, 09 minutes
Location:	N/A
Contact:	N/A
Router IP Address:	192.168.159.21
SNMP Read-Write Community String:	XXXXXXXXXX
Verify String:	XXXXXXXXXX
<div>Test Apply Reset</div>	

Host Parameters - SNMP

During installation of the NAM-1/2, the NAM is made aware of the SNMP community strings set of the host switch allowing for the retrieval of mini-RMON information. However, in the case of the NM-NAM, you must configure the NM-NAM with the community strings configured on the host access router to allow the NM-NAM to retrieve the MIB-II interface, router health, and NBAR-PD statistics from the router's SNMP agent. To do so, enter the Cisco access router's read-write community strings in the *Setup > Router Parameters > Router Information* submenu.

Getting Started

Host Parameters - NBAR

Setup > Switch Parameters > NBAR Protocol Discovery
Setup > Router Parameters > NBAR Protocol Discovery

NBAR Status

Current Status: Partially Enabled

NBAR is activated on a subset of interfaces, and the NAM can provide NBAR statistics for these interfaces. Other interfaces may not have the NBAR feature enabled. You can use the 'Details' button to view more detailed interface information, and if necessary, click the 'Enable' button to activate NBAR on all switches.

This can have an impact on the switch performance.

Details Save Enable Disable

Current NBAR status

NBAR status per interface

Note: The NBAR Protocol Discovery feature is not available on all versions of switch software

- NBAR is a feature that must be enabled for the NAM to display information about protocols discovered on each interface using the menus:
 - Monitor > Switch > NBAR or
 - Monitor > Router > NBAR
- Click the 'Enable' button to turn on NBAR for all eligible interfaces.

NBAR Interface Details

Interface Name Filter Clear

Showing 1-15 of 25 interfaces

Interface	Interface Type	NBAR Enabled
Fa0/0	ethernetCsmacd	✓
Se0/0	frameRelay	✓
Fa0/1	ethernetCsmacd	✓
Se0/1	ppp	✓

Rows per page: 15 Go to page: 1 of 2 Go

Close

Host Parameters – NBAR

The NBAR-PD (Network-Based Application Recognition – Protocol Discovery) MIB is used to collect statistics on all protocols (applications) seen on an interface. This feature can be useful for collecting application information on interfaces that are not being monitored by the NAM, thus increasing overall application visibility. However, it should be noted that NBAR-PD can have an impact on the performance of a device, especially a switch with many ports.

Use the **Setup > Switch/Router Parameters > NBAR Protocol Discovery** task to check on the current NBAR collection status. This task also allows the administrator to enable/disable NBAR on all eligible interfaces and view the details of NBAR collection for each interface. NBAR collection changes take place immediately on Catalyst OS devices, but the **Save** button must be used for the changes to take effect on IOS devices.

Note: The NBAR Protocol Discovery feature is not available on all versions of switch software.

Getting Started

Host Parameters – Mini RMON

NAM-1, NAM-2 Only

Setup > Switch Parameters > Port Stats (Mini-RMON)

Port Stats (Mini-Rmon)

Current Status: Enabled

The NAM is currently able to provide Port Stats with this configuration.
No further action is necessary.

Details Save Enable Disable

Current Mini-RMON status on switch

Mini-RMON status per switch port

- Mini-RMON is a switch feature that must be enabled for the NAM to provide useful information about Ethernet ports on the **Monitor > Switch > Port Stats** screen.
- Click the 'Enable' button to turn on Mini-RMON for all eligible Ethernet ports.

Port Stats (Mini-Rmon) Details

Port Name Filter Clear

Note: Typically only ethernet interfaces can have Mini-Rmon. Other interfaces such as WAN interfaces can not.

Showing 1-10 of 66 port interfaces

Port Name	Port Type	Mini-Rmon Enabled
Gi1/1	ethernetCsmacd	✓
Gi1/2	ethernetCsmacd	✓
Gi1/3	ethernetCsmacd	✓
Gi1/4	ethernetCsmacd	✓

Rows per page: 10 Go to page: 1 of 7 Go Close

Host Parameters – Mini-RMON

Typically the starting point for any monitoring effort is to determine the utilization and health of an individual segment. In the case of a switch, this means determining this for every port. Ports exhibiting unusual behavior can then be Spanned to the NAM for more in-depth analysis. Every Catalyst Switch collects Mini_RMON (a subset of RMON I) statistics for every port which the NAM can then retrieve and display. The **Setup > Switch Parameters > Port Stats** task can be used to determine the status of Mini-RMON collection for the switch, as well as each individual port. This task also allows the administrator to enable/disable Mini-RMON on all eligible interfaces. Mini-RMON collection changes take place immediately on Catalyst OS devices, but the **Save** button must be used for the changes to take effect on IOS devices.

Getting Started

Host Parameters – Switch Login

NAM-1, NAM-2 Only

The NAM allows you to collect RMON 2 statistics per MPLS VRF, VCID, or Label. To automatically retrieve this information from the switch, you must first provide the NAM with the access credentials for the switch

The screenshot shows the NAM Traffic Analyzer web interface. The top navigation bar has tabs for Setup, Monitor, Reports, Capture, Alarms, and Admin. The left sidebar shows a tree view with 'Switch Login' selected. The main content area is titled 'Switch Login Configuration' and contains fields for User Name, Password, Verify Password, and Login Method (Telnet/SSH). A 'Test Login' button is also present. An 'Instructions' panel on the right explains the requirements for enabling the MPLS monitoring feature.

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-49

Host Parameters – Switch Login

As we will see shortly, the NAM allows you to break down SPANned traffic into VLANs and thus get statistics on a per VLAN basis. Similarly, the NAM can break down SPANned traffic into individual MPLS streams (LSPs, VCID, Labels). To know which MPLS streams are available, the NAM logs into the device and issues the following IOS commands to retrieve the information:

- show ip vrf - get all VRF/VC configured
- show mpls forward-table vrf - get MPLS local labels with each VRF/VC
- show ip cef vrf name detail - get all egress labels associated with a VRF
- show mpls l2transport vc vcid detail - get all egress labels for a VC

Of course, in order to issue these commands, the NAM must have the access credentials to log into the device. The **Setup > Switch Parameters > Switch Login** task is used to provide the NAM with the Telnet login information for the device. The enable password is not required.

Getting Started

Audit Trail - Enabling

The screenshot shows the NAM Traffic Analyzer web interface. The top navigation bar includes links for Help, Logout, and About. Below this is a menu with tabs: Setup, Monitor, Reports, Capture, Alarms, and Admin. The Admin tab is selected, and the Preferences sub-tab is also selected. The main content area displays the Preferences configuration page. A table lists various settings, including Entries Per Screen, Refresh Interval, Number Graph Bars, Perform IP Host Name Resolution, Data Displayed in, Format Large Numbers, International Notation, CSV Export Monitor Entries, and Audit Trail. The Audit Trail checkbox is checked and circled in red. The Apply and Reset buttons are also circled in red. A yellow callout box on the left states: 'The Audit Trail provides useful information such as which user logged in, from what IP address, and what activities were performed during that session.'

Preferences	
Entries Per Screen (1-1000):	50
Refresh Interval (15-3600 sec):	60
Number Graph Bars (1-15):	10
Perform IP Host Name Resolution:	<input checked="" type="checkbox"/>
Data Displayed in:	<input checked="" type="radio"/> Bytes <input type="radio"/> Bits
Format Large Numbers:	<input type="checkbox"/>
International Notation:	<input checked="" type="radio"/> 1,025.72 <input type="radio"/> 1.025,72 <input type="radio"/> 1 025,72
CSV Export Monitor Entries:	<input type="radio"/> All <input checked="" type="radio"/> Current Screen Only
Audit Trail:	<input checked="" type="checkbox"/>

Apply Reset

Enabling Audit Trail

When you have finished configuring the NAM for secure and functional access, you can track critical web GUI and CLI user activities in an audit log to enhance security. To enable the Audit Trail, select Admin > Preferences and check Audit Trail. Shortly we will see how to configure the NAM to forward audit trail alerts as syslogs to a remote system.

Getting Started

Audit Trail - Viewing

CISCO SYSTEMS

NAM Traffic Analyzer

Setup Monitor Reports Capture Alarms **Admin**

Users System **Diagnostics**

You Are Here: Admin > Diagnostics > Audit Trail

Audit Trail

Current Data: as of Thu 07 Sep 2006, 17:43:34 UTC

Time	User	From	
07 Sep 2006, 16:52:13	admin	10.21.89.164	User login
07 Sep 2006, 15:06:21	admin	10.70.230.54	User login
07 Sep 2006, 14:33:27	admin	144.254.200.222	User login
07 Sep 2006, 07:34:57	admin	64.104.5.212	Report created: Top-Apprication
07 Sep 2006, 07:19:37	admin	64.104.5.212	Report created: N
07 Sep 2006, 07:18:53	admin	64.104.5.212	Report created: T
07 Sep 2006, 07:17:30	admin	64.104.5.212	User login

The Access Log provides useful information such as which user logged in, from what IP address, and what activities were performed during that session.

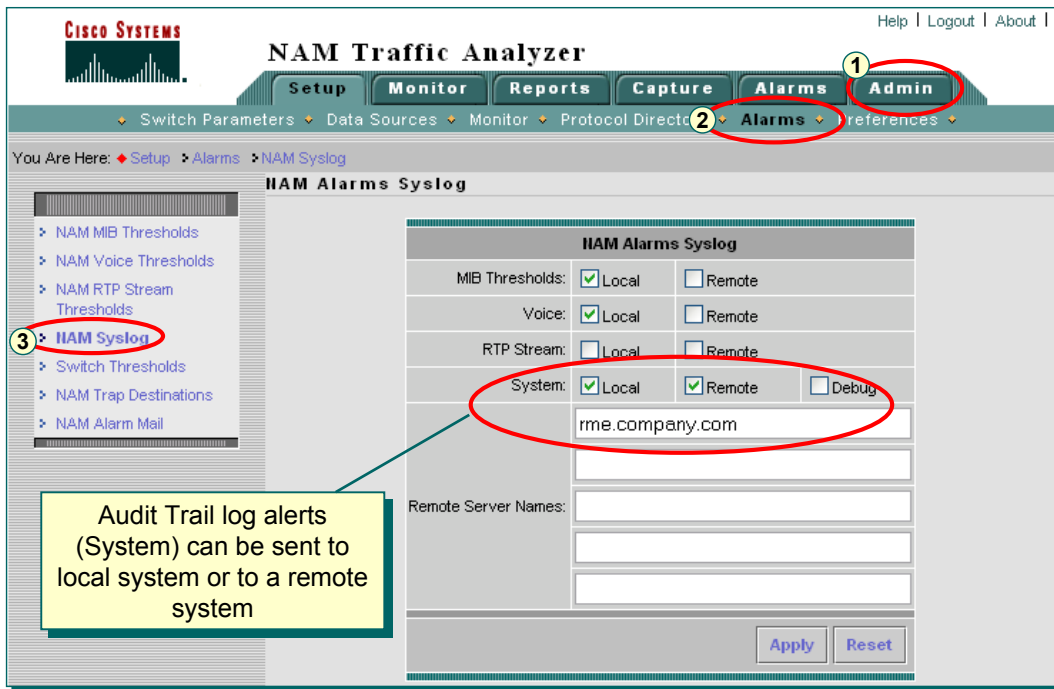
Viewing Audit Trail

The audit trail provides the following type of information by user ID, time, IP address of access point, and brief description:

- All CLI commands performed
- User logins, including failed attempts
- Unauthorized access
- SPAN setup changes
- NDE Data Source changes
- Enable/Disable Data Collections
- Create/Delete Reports
- Start/Stop Captures
- Add/Delete Users

To view the audit trail log, go to the **Admin > Diagnostics > Audit Trail** task.

Audit Trail – Sending as Alerts



Sending Audit Alerts as Syslogs

The NAM provides the capability to send audit alerts as Syslog messages to a remote system. To configure this feature select the **Admin > Alarms > NAM Syslog** task. Enable the local and/or remote check box for the System entity. If remote was checked then you must also enter the remote servers name.

We will revisit this screen later when discussing the dissemination of NAM alarms for MIB, Voice, and RTP stream threshold violations.

Getting Started

Setting NAM System Time

CISCO SYSTEMS NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Users System Diagnostics

You Are Here: Admin System NAM System Time

NAM System Time

System Resources
Network Parameters
NAM SNMP
NAM System Time
E-Mail Configuration
FTP Configuration
Capture Data Storage
Web Publication

NAM System Time Configuration

Current NAM System Time: Thu 07 Sep 2006, 17:46:26 UTC

Synchronize NAM System Time With: ☒ Switch ☐ NTP Server

NTP Server Name/IP Address:

NAM local time zone: Region Zone

Apply Reset

Instructions

Configure the NAM system time to synchronize with either the local switch/router or external NTP servers. If NTP is used for time synchronization, enter a minimum of one NTP server name or IP address. You must configure the NAM's local time zone regardless of the time synchronization method.

Configure the NAM system time to either synchronize with the time set on the host switch or configure the NAM to set its time based on an NTP server.

Setting NAM System Time

Before setting the NAM up for monitoring and reviewing the results, it should be noted that most analysis of the data reported by the NAM will often be dependent upon the time the events reported occurred. Therefore it is important that the time of the NAM is properly set. The system time of the NAM can be either synchronized with the time set on the host device or can be retrieved and set from an NTP server responsible for setting the time on all network devices.

Getting Started

E-mail Configuration

CISCO SYSTEMS NAM Traffic Analyzer

Help | Logout | About

Setup Monitor Reports Capture Alarms Admin

Users System Diagnostics

You Are Here: Admin > System > E-Mail Configuration

E-Mail Configuration

Mail Configuration

Enable Mail: ☒

External Mail Server: smtp.outgoing.com

Send Test Mail to: admin@company.com

Apply Reset

Instructions

To enable Email support, an external Email server must be configured. This is the POP or exchange mail server for your organization. To validate the mail configuration, a complete email address, such as jdoe@cisco.com, can be entered to receive a test email when NAM completes the configuration.

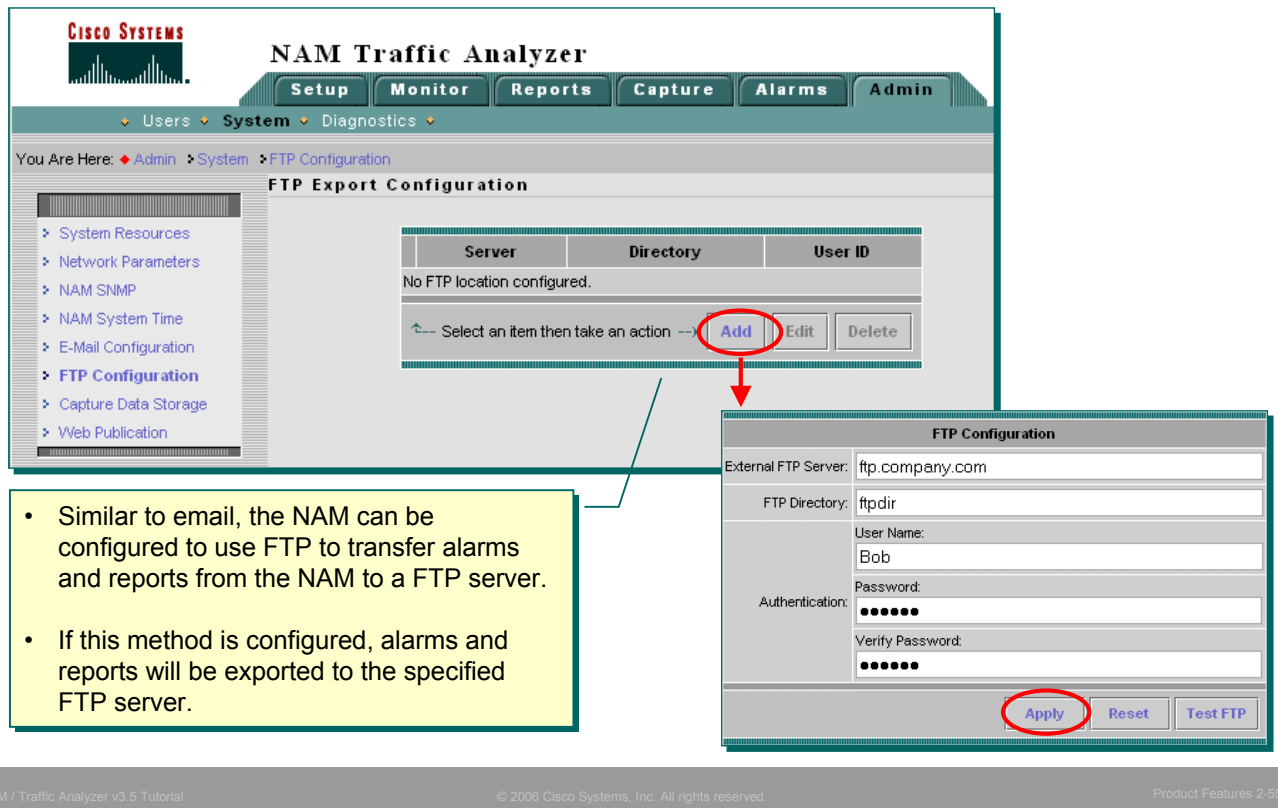
The NAM can be configured to send e-mail notification of alarms as well as e-mail reports. Use this configuration screen to configure the e-mail server

E-mail Configuration

The NAM allows both alarms and reports to be disseminated via e-mail. Use the **Admin > System > E-mail Configuration** task to define the external mail server (pop or exchange) to be used.

Getting Started

FTP Configuration



The screenshot shows the NAM Traffic Analyzer web interface. The breadcrumb trail is **Admin > System > FTP Configuration**. The main content area is titled "FTP Export Configuration" and contains a table with columns "Server", "Directory", and "User ID". The table is empty, with the text "No FTP location configured." below it. Below the table is a dropdown menu with the text "Select an item then take an action --" and three buttons: "Add", "Edit", and "Delete". The "Add" button is circled in red. A red arrow points from the "Add" button to a detailed "FTP Configuration" dialog box. This dialog box contains the following fields:

- External FTP Server: ftp.company.com
- FTP Directory: ftpdir
- User Name: Bob
- Password: (masked with dots)
- Verify Password: (masked with dots)

At the bottom of the dialog box are three buttons: "Apply", "Reset", and "Test FTP". The "Apply" button is circled in red.

- Similar to email, the NAM can be configured to use FTP to transfer alarms and reports from the NAM to a FTP server.
- If this method is configured, alarms and reports will be exported to the specified FTP server.

NAM / Traffic Analyzer v3.5 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-55

FTP Configuration

The NAM also allows reports and alarms to be transferred via FTP. Use the **Admin > System > FTP Configuration** task to add external ftp servers, their access credentials, and the directory to place the reports in.

Getting Started

Web Publishing

The screenshot shows the NAM Traffic Analyzer web interface. At the top, there's a Cisco Systems logo and navigation links: Help, Logout, About. Below the logo is a bar with tabs: Setup, Monitor, Reports, Capture, Alarms, Admin. A breadcrumb trail shows: Users > System > Diagnostics > Web Publication. The main content area is titled 'Web Data Publication' and contains a section 'Enable Web Data Publication' with a checked checkbox. Below this, there are checkboxes for 'Monitoring pages except Voice', 'Voice Monitoring pages', 'Reports', and 'Alarms pages'. There are also input fields for 'Publication Code (optional)' and 'ACL (optional) permit IP addr/subnets:'. At the bottom right of this section are 'Apply' and 'Reset' buttons. On the right side, there's an 'Instructions' box with text explaining web publication. On the left, a navigation menu lists various system resources, with 'Web Publication' highlighted. A yellow callout box with a green border points to the 'Web Publication' link in the menu, containing the text: 'Configure the NAM to allow web users to view various reports without having to establish a login session with the NAM'.

Configure the NAM to allow web users to view various reports without having to establish a login session with the NAM

Web Data Publication

☒ **Enable Web Data Publication**

Publish:

- ☒ Monitoring pages except Voice
- ☒ Voice Monitoring pages
- ☒ Reports
- ☐ Alarms pages

Publication Code (optional):

ACL (optional) permit IP addr/subnets:

Instructions

Web publication allows general web users and web sites to access (or link to) selected NAM monitor and report screens without a login session.

Publication can be open or restricted using Access Control List (ACL) and/or publication code. The publication code, if required, must be present in the URL address or cookie to enable access to published data.

Web Publishing

You can enable the NAM to allow general web users to view reports without having to establish a login session with the NAM or to publish the reports on other web sites. To enable this feature, select **Admin > System > Web Publication**, select the report types to publish on the web, and optionally restrict access using a Publication Code and/or Access Control List (ACL).

CISCO SYSTEMS



Network Monitoring Using NAMs

NAM Hardware Overview

➤ **Traffic Analyzer Software**

- Planning
- Getting Started
- **Configuring**
- Viewing Reports
- Packet Capture and Decode



- **Basic NAM-1, NAM-2 Configuration**

- Overview of Steps
- Configuring Data Sources
- Enabling Core Monitoring

- **Basic NM-NAM Configuration**

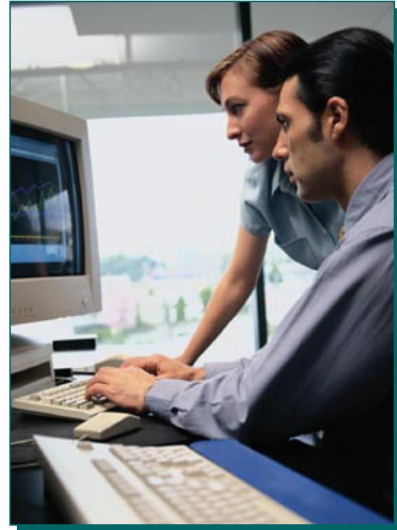
- Overview of Steps
- Configuring Data Sources
- Enabling Core Monitoring

- **Types of Statistics Collected**

- **Enabling Traffic Monitoring**

- **Configuring Alarms**

- **Setting Preferences**



Monitoring Setup and Configuration

All the work thus far has involved building the foundation for this next section, configuring the NAM for monitoring. Monitoring refers to all the functions that the NAM includes to provide you with more visibility into your network. Monitoring refers not only to the passive process of collecting data for review and analysis but also to the proactive process of creating alarms to notify you when an event occurs on your network that you want to know about. Monitoring configuration consists of several steps:

1. **Configuring data sources:** For the NAM-1/2 includes configuring the switch to mirror data from ports, VLANs, or the Cisco EtherChannel® tunnel to the NAM data port (SPAN/VACL); or for the NM-NAM configuring CEF on interfaces to forward packets to the internal NAM port; also for both types of NAMs configuring NetFlow devices to send flow statistics to the NAM. This step provides the data streams for analysis and reporting
2. **Configuring monitoring parameters:** Instructing the NAM on what data (statistics, hosts, conversations, application response time, DiffServ, VoIP) to collect from the configured data sources and how it should be analyzed and reported
3. **Configuring alarms:** Configuring thresholds and alarms based on the data sources you configured in Step 1
4. **Configuring traps:** Configuring the NAM to send traps to a management station for proactive notification of events that occur
5. **Preferences:** Configuring the presentation of data and reports that you view under Monitor

The following section walks you through each of these steps, to lay the foundation for both passively and proactively monitoring your network. This section shows you both the menus that you will use to configure the NAM as well as sample reports that show you what effect your configuration choices have on the presentation of data.

Basic NAM-1/2 Configuration Overview of Steps

NAM-1, NAM-2 Only

Step 1 – Defining the Data Sources

- **SPAN Session** → Data Port
- **RSPAN Session** → Data Port
- **VACL** → Data Port
- **NetFlow Data Export (NDE)** → NDE Data Port
- **MPLS (import VRF, VCID, Labels)**
- Supervisor Module (enable Mini-RMON)

Step 2 – Enabling Core Monitoring

- Turn on various types of statistics for different traffic sources seen by the NAM
- Traffic Sources:
 - **ALL SPAN** (if multiple span sessions exist)
 - **Data Port** (if using a NAM-2 module, specify which Data Port (1 or 2))
 - **Individual VLANs**
 - **MPLS (VRF, VCID, Labels)**
 - **NDE traffic** (All or a subset)
 - **ERSPAN**
 - **Supervisor** (mini-RMON, VLAN stats)
- For each data source, different types of statistics can be enabled (Protocol, Hosts, Conversations, VLAN statistics)

Basic NAM-1/2 Configuration – Overview of Steps

One of the keys to a successful NAM deployment is properly selecting and configuring data sources. The user must understand that this is a two step process. First, data must be sent to the NAM for analysis, and secondly, several monitoring options must be enabled for various subsets of the traffic sent to the NAM for analysis.

Data can be sent to the NAM-1/2 for analysis using the following methods. (Each of these will be discussed in greater detail in the upcoming pages.)

- Spanning ports, VLANs, or Ether Channels to a NAM-1/2 data port; the NAM-2 has two data ports.
- VACL – Use the command line of the switch to forward packets from an interface.
- NDE – Forward NetFlow packets from a device to a special interface on the NAM-1/2.

At this point the data is being sent to the NAM, but not yet being analyzed. The second step is to turn on various monitoring options (Enabling Monitoring) for different subsets of the forwarded traffic. The data sources provide the traffic to the NAM for analysis. The traffic is analyzed and broken down into subsets of traffic (all traffic, individual VLANs, individual MPLS tags, or subsets of NDE sources). The user will then configure the NAM to monitor various types of statistics (applications, protocols, hosts, conversations, etc.) for these traffic sources.

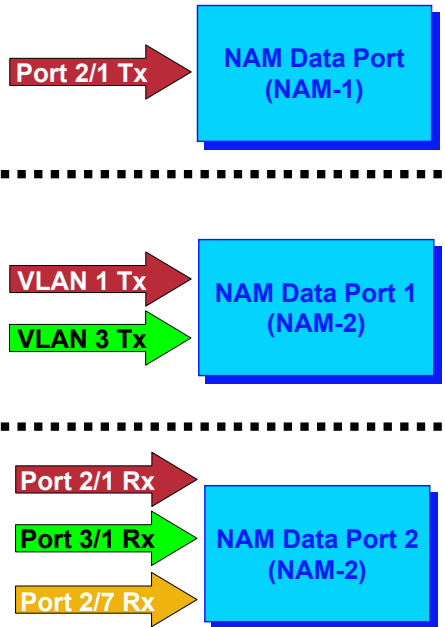
TIP: Often times, if a report does not display any data, this can always be traced back to one of the following configuration scenarios:

- The requested data is not currently being spanned to the NAM-1/2, but the subset of traffic is still enabled.
- The requested data is currently being spanned to the NAM-1/2, but the subset of traffic is not enabled.

Step 1: Configuring SPAN / RSPAN Data Sources

Examples

1. Types of SPAN / RSPAN Sessions
 - a. One or more ports from various modules
 - b. One or more VLANs
 - c. Single RSPAN VLAN
 - d. One or more Ether Channels
2. If source is a port, first select switch module where port is located
3. If NAM-2, specify SPAN destination Data Port (1 or 2); One type of SPAN session per Data Port
4. If Port, VLAN, or Ether Channel select the direction of traffic to send to the NAM
5. Select the actual source (Ports, VLANs, Ether Channels) to send to the NAM



Configuring SPAN / RSPAN Data Sources

You have the option of choosing ports, VLANs, or Cisco EtherChannel® tunnels as a SPAN source. The importance of defining your SPAN source is tied implicitly to what problem you are trying to solve or how you want to view the data. For example, if you choose to use SPAN on a port, then all graphs, tables, and charts will be derived from the data that the NAM collects on the port(s) you have spanned. Furthermore, you will be able to view VLAN information only for VLANs that are active on the spanned port(s). If you are more interested in how your VLANs consume switch and network resources, then choosing VLAN spanning will provide you with charts and statistics by the VLANs you have spanned. The same is true for Cisco EtherChannel tunnel.

Once the type of SPAN has been selected, the user further configures additional parameters:

- If spanning ports, first select the switch module where the port(s) are located; then select the port(s) you wish to span from a list.
- If a NAM-2 module is being utilized, select the data port to SPAN this traffic to.
- Select the direction of traffic you want to monitor—transmitted (Tx), received (Rx), or both (*bi-directional*). Since packets can be counted twice, you may want to review the spanning concepts covered earlier in this chapter or in the references in Chapter 5 before choosing or changing the default parameters on direction.
- Select the actual ports, VLANs, or Ether Channels to be spanned.

Note(s):

- *When spanning any source, it is important to keep in mind the volume of traffic that your SPAN session generates, because this will affect the overall performance of the NAM and the reliability of your data.*
- *When spanning Rx ports, many can be selected. When spanning Tx or bi-directional ports, only one can be selected. For VLANs, it doesn't matter.*

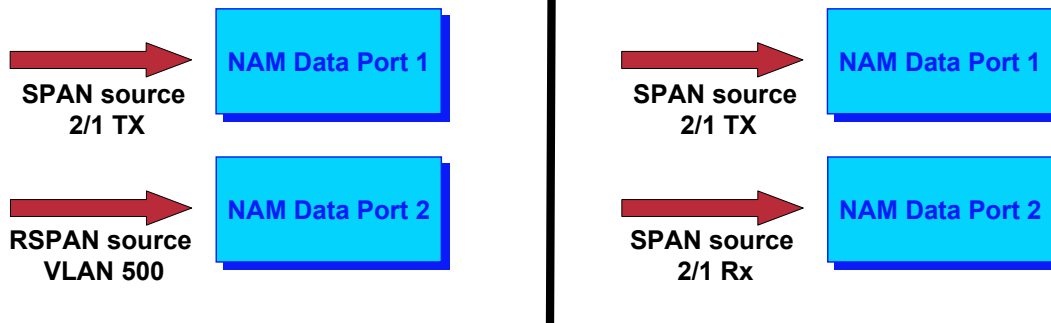
Basic NAM-1/2 Configuration

NAM-2 Only

Step 1: Utilizing the Second Data Port on NAM-2

- Must specify which data port to send traffic (Data Port 1 or Data Port 2)
- Can have 2 simultaneous SPAN / RSPAN / VACL sessions
 - Cannot mix types of sessions on same data port
- Use the 2 ports independently or together; for example:
 - Dedicate one data port for reporting, the other for troubleshooting
 - Break out in/out traffic by spanning to each port in one direction

Examples



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-61

Utilizing the Second Data Port on NAM-2

Besides the increased processing and memory performance of the NAM-2, it also includes a second data port for increased flexibility when selecting data sources for monitoring. This allows for many different possible uses including:

- Using one port for troubleshooting and dedicating the other to historical reporting
- Breaking out the traffic direction for finer granularity monitoring (one port for transmitted data, and one port for received data)
- Increased flexibility when choosing data sources:
 - 2 SPAN sessions
 - 1 SPAN, 1 RSPAN
 - 1 SPAN, 1 VACL
 - Etc.

Note: If using 2 VACL sessions, the SPAN active window will not display any active sessions, yet data is currently being sent to the NAM-1/2. Always review the host switch configuration to determine if any VACLs are forwarding data to the NAM.

Basic NAM-1/2 Configuration

Step 1: Configuring SPAN / RSPAN Data Source

CISCO SYSTEMS NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Switch Parameters Data Sources Monitor Protocol Directory Alarms Preferences

You Are Here: Setup > Data Sources > SPAN

Active SPAN Sessions

Monitor Session	Type	Source - Direction	Dest. Port	Dest. Module	Status
1	port	1/1 - Rx 1/2 - Rx 1/7 - Rx down 1/8 - Rx down	3/7	3 (local)	active

Select a SPAN session, then take an action-->

Create Save Add Dest. Port 1 Add Dest. Port 2 Edit Delete

Continued

- Shows one active SPAN sessions; NAM is in slot 3. DataPort1 is 3/7.
- Click **Create** to define new session. If there are no available DataPorts then one would need to be deleted first.
- If using a NAM-2, a second active session can be defined on DataPort 2 (port 3/8).

Configuring SPAN / RSPAN Sources

To SPAN data to the NAM-1/2 for analysis first select the **Setup > Data Sources > SPAN** task (This task will not be displayed on an NM-NAM). A table will be displayed showing the active SPAN sessions. This screen is also useful to refer to when first accessing the NAM-1/2 to verify what the current NAM-1/2 data sources are, in case they were changed since you last used the Traffic Analysis software.

If a SPAN session is already active, another one cannot be created (unless a NAM-2 is being utilized) until the current session has been deleted. Another option is to **Edit** the current session, but only if the SPAN type is not to be changed.

Note(s):

- The Active SPAN window will display all SPAN sessions on the host switch and not just the NAM related SPAN sessions.
- Select **Create** to start a new SPAN session. (Refer to next page.)

Basic NAM-1/2 Configuration

Step 1: Configuring SPAN / RSPAN Data Source

Create SPAN Session

Monitor Session: 2

SPAN Type: ☐ Switch Port ☒ VLAN ☐ EtherChannel ☐ RSPAN VLAN

Switch Module: Not Applicable

SPAN Destination Interface: DATA PORT 2

SPAN Traffic Direction: ☐ Rx ☒ Tx ☐ Both

Available Sources:

- default (1)
- VLAN0002 (2)
- VLAN0032 (32)**
- fdi-default (1002)
- token-ring-default (1003)
- fdinet-default (1004)
- trnet-default (1005)

Selected Sources:

- VLAN0032 (32) (Tx)

Buttons: Add, Remove, Remove All, Submit

Span sessions can consist of one or more ports or VLANs, but not a mix of ports and VLANs

Configuration screen for creating a SPAN session. Configurable options include:

- SPAN type (port, VLAN, EtherChannel, RSPAN VLAN)
- Switch module, if spanning ports
- SPAN destination interface (NAM-2 only),
- SPAN direction, and
- SPAN sources

Configuring SPAN / RSPAN Sources

If you have selected **Create** to start a new SPAN session on the **Setup>Data Sources>SPAN** dialog window, follow these steps:

- Select the SPAN type and other parameters to configure the SPAN session and select Submit when finished. The traffic selected for the SPAN session is now being forwarded to the NAM-1/2 for monitoring. Remember, no monitoring takes place until the data sources have been enabled for monitoring. Before enabling the monitoring, let's first look at the configuration process for the other types of data sources.
- Before **RSPAN data sources** will be displayed when selecting the RSPAN radio button, the user must first configure the source switch with an RSPAN VLAN and the source ports, and also configure the NAM host switch with the RSPAN VLAN number.
- When the host switch is running Cisco IOS software, the SPAN session dialog box includes a pull down menu to set the monitor session number. When using CatOS, the session id is automatically selected and tracked.

Basic NAM-1/2 Configuration

Step 1: Configuring VACL Data Source

VACL are valuable data source for:

- Analyzing WAN Ports (packets forwarded as Ethernet frames)
- Analyzing LAN interfaces if all SPAN sessions are in use
- Pre-filtering traffic before sending it to the NAM



NAM Data Port 1

```
6509 (config) #access-list 100 permit ip any any
6509 (config) #vlan access-map wan 100
6509 (config-access-map) #match ip address 100
6509 (config-access-map) #action forward capture
6509 (config-access-map) #exit
6509 (config) #vlan filter wan interface ATM6/0/0.1
6509 (config) #analysis module 3 data-port 1 capture allowed-vlan 1-4096
6509 (config) #analysis module 3 data-port 1 capture
```

Configured from host switch CLI

Configuring VACL Data Source

As mentioned earlier, VACLs are useful for several applications: monitoring IP traffic from WAN ports, analyzing LAN interfaces if all the SPAN sessions are in use, or for pre-filtering traffic before sending it to the NAM for further analysis. The use of VACLs to copy traffic to the NAM for monitoring purposes requires configuration from the host switch CLI.

The above example shows how to configure a VACL on an ATM WAN interface and forward both ingress and egress traffic to the NAM. These commands are for switches running Cisco IOS version 12.1(13)E1 or higher. For LAN VACLs on Catalyst OS, the security Access Control List (ACL) feature can be used to achieve the same result.

Refer to the NAM User Guide for more examples or the Switch Command Reference for more details on using and configuring VACLs.

Basic NAM-1/2 Configuration

Step 1: Configuring MPLS

CISCO SYSTEMS

NAM Traffic Analyzer

Setup Monitor Reports Capture Alarms Admin

Switch Parameters Data Sources Monitor Protocol Directory Alarms Preferences

You Are Here: Setup > Data Sources > MPLS > L3 VRF

MPLS VRF Data Source Configuration

VRF-Label Mapping: Import from Router Import from File Export to File Import Log

VRF Name	Local Label	Egress Label	Data Source
customer_A	102	207/304	VRF:customer_A
customer_B	103	207/305 207/306	VRF:customer_B

Select an item then take an action --> Create DataSrc Delete DataSrc

Import VRF configurations from the device hosting the NAM

Import VRF configurations from a file

Select VRF and click Create Data Source to be able to monitor VRF

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-65

Configuring MPLS

This step is unique in that we are not actually defining a data source, but rather prepare to define the subset of the data source that we wish to monitor.

As previously mentioned, the NAM can analyze all or a subset of the traffic sent via a SPAN session to the NAM. One such subset is MPLS traffic streams. The NAM can monitor individual MPLS traffic streams at layer 3 by using the VRF's mapping to MPLS labels as the defining factor or at Layer 2 using the VCID's mapping to MPLS labels as the defining factor.

This information is either imported from the router (requires the **Setup > Switch Parameters > Switch Login** task to be completed) or imported from a file.

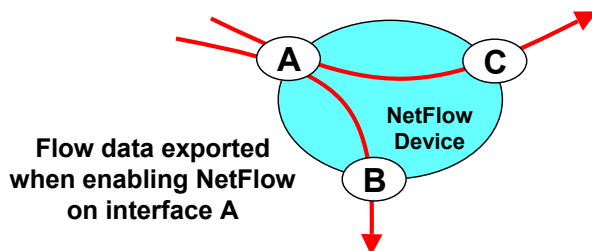
Once a list of VRFs and/or VCIDs are listed, select the desired entry, and click the **Create DataSrc** button. This will create a data sources for this MPLS traffic stream that can be configured for monitoring (see step 2 - enabling Core Monitoring).

Basic NAM Configuration

Step 1: NetFlow Data Sources

Same for NAM-1, NAM-2, and NM-NAM

1. Configure NetFlow device to forward to NAM on UDP port 3000
2. Use Listening Mode to see who is sending NAM NDE traffic
3. Add NetFlow Device
 - a. Automatically creates NDE data source for all forwarded traffic
 - b. Alternatively create custom NDE data source for subset of all forwarded NDE traffic



NDE packets are received by the NAM-1/2 on a separate internal NAM interface, and on the NM-NAM interface configured as the management interface

- NetFlow Data Sources do not support all NAM monitoring features.
- Supported features – Applications, Hosts, Conversations, and DiffServ

Configuring NetFlow Data Sources

NetFlow Data Export is an alternative way to monitor local/remote WAN traffic on either type of NAM. NDE monitoring can provide application, host, and conversation information for either the local device or remote NetFlow enabled devices that have been configured to forward NDE packets to the NAM on UDP port 3000. In its simplest form, NDE provides an aggregate view of traffic flow through a device at layer 3. However, with more complex configurations, NDE records can be bundled by interface and direction. See the Command Guide for the NetFlow device for more information on NetFlow and its configuration.

Once NDE packets are being forwarded to the NAM by a remote device, the NAM must add that device before packets will be considered for monitoring. This step is similar to setting up a SPAN session. (The user can also optionally create custom NDE data sources for a subset of the NDE flow from a device.) Like any NAM data source, the NDE data sources at this point are only being accepted by the NAM, no processing of packets takes place until monitoring is enabled for the individual data sources. This step will be covered in detail later in this chapter, but first let's look at the details of configuring NDE data sources on the NAM.

Note(s):

- NDE packets are received by the NAM-1/2 on a the internal NAM management interface
- NDE packets are received by the NM-NAM on the management interface. See Chapter 4 or the NM-NAM Installation Guide for more on configuring the NM-NAM interfaces.

Basic NAM Configuration

NetFlow Listening Mode

Same for NAM-1, NAM-2, and NM-NAM

To create NDE data sources, the NetFlow device sending NDE packets to the NAM must be entered into the NAM NDE device table. Use the listening mode to determine which devices are forwarding NDE packets to the NAM

Start the listening mode

Setup > Data Sources > Listening Mode to select Listening mode

Add Device

View NDE details (NetFlow enabled interfaces)

Address	Number Received NDE Packets	Last Packet Received
127.0.0.11	106	Tue 17 Jun 2003, 11:43:24 Pacific
192.168.76.2	393	Tue 17 Jun 2003, 11:43:36 Pacific
192.168.76.4	106	Tue 17 Jun 2003, 11:43:24 Pacific
192.168.79.102	136	Tue 17 Jun 2003, 11:43:35 Pacific
192.168.79.110	103	Tue 17 Jun 2003, 11:43:31 Pacific

Device Added	Interfaces Reported in NDE Packets
No	Special (0) (Output) (1) (Input) (6) (Output) (9) (Output)

NetFlow Listening Mode

The first step in using NDE packets for monitoring purposes is to configure the NetFlow device (local or remote) to forward them to the NAM (remember the NAM is assigned an IP address during installation). Next, the NetFlow devices must be added to the NAM, which creates a default NDE data source for that device. But what devices were configured to send NDE to the NAM? Use the NetFlow Listening Mode task to display all devices sending NDE packets to the NAM whether or not they have been added to the NAM NetFlow device table.

Launch the NetFlow Listening Mode by selecting **Setup > Data Sources > NetFlow > Listening Mode** and clicking the **Start** button on the Listening Mode table. Assuming *Auto Refresh* is selected, the table will periodically update (listening mode will automatically stop after 1 hour) to display the devices the NAM is receiving NDE packets from.

Highlight one of the devices and select **Details** to view the interfaces reported in the packets and whether or not the device has been added to the NAM NetFlow table. If the device has not been added to the NAM NetFlow table, highlight the device and select the **Add** button. A new dialog will query the user for the device Read community string to retrieve the text string interface designations. Adding the device to the NDE table creates a default NDE data source, which can be used to monitor the aggregate of all enabled flows on the device. Subsets of all flows (i.e. single interface) can also be monitored by creating custom data sources, as will be discussed shortly.

Remember, to create a NDE data source the device must be added to the NAM NetFlow table.

Note: Once the device is added to the NAM NetFlow device table with the associated Read community string, the details window will also display the text string interface designation and not just the interface index number.

Basic NAM Configuration

Defining NetFlow Devices

Same for NAM-1, NAM-2, and NM-NAM

CISCO SYSTEMS

NAM Traffic Analyzer

Help | Logout | About |

Setup | Monitor | Reports | Capture | Alarms | Admin

Switch Parameters | Data Sources | Monitor | Alarms | Preferences

You Are Here: Setup > Data Sources > NetFlow Devices

NetFlow Devices

	Address	Community String
<input type="radio"/>	127.0.0.11 (local switch)	*****
<input type="radio"/>	192.168.76.2	*****
<input type="radio"/>	192.168.78.5	*****
<input type="radio"/>	192.168.79.102	*****

Test Create Edit Delete

Instructions: The Test button is available to test the connectivity of the device.

Test connectivity of device

New Device

Device: 192.168.79.110

Read Community String: *****

Verify Community String: *****

OK Reset Cancel

NetFlow Devices

Besides adding devices from the Listening Mode window, devices can be added/edited/deleted at any time using the **Setup > Data Sources > NetFlow > Devices** task. Additionally, if monitoring reports are not showing any data, first refer to this list and highlight the suspect device and click the **Test** button to verify connectivity.

Once the device is added, the NAM creates a default NDE data source for all the flows from this device. Next let's discuss how to create an NDE data source that is specific to certain interfaces on the device.

Basic NAM Configuration

NetFlow Custom Data Sources

Same for NAM-1, NAM-2, and NM-NAM

NAM Traffic Analyzer

Setup Monitor Reports Capture Alarms

Switch Parameters Data Sources Monitor Alarms Preferences

You Are Here: Setup > Data Sources > NetFlow Custom Data Sources

NetFlow Custom Data Sources

	Data Source Name	NDE Device	Interfaces
default	NETFLOW	127.0.0.11	Any
<input type="radio"/>	NDE-127.0.0.11:1/2 (4) (Input)	127.0.0.11	1/2 (4) (Input)
<input type="radio"/>	NDE-Test	127.0.0.11	VLAN-1 (5) (Both) VLAN-1002 (6) (Both) VLAN-1004 (7) (Both)
default	NDE-192.168.76.2	192.168.76.2	Any
default	NDE-192.168.79.102	192.168.79.102	Any
<input type="radio"/>	NDE-WAN	192.168.79.102	Fa0/0 (1) (Both) Se4/0 (4) (Both)
default	NDE-192.168.79.110	192.168.79.110	Any

←--Select an item then take an action -->

Create Edit Delete

Instructions

To optionally create a custom data source, you can click the Create button.

The default data sources, which were created automatically when you created a device, cannot be edited or deleted.

Create new NDE data source (See next page)

NetFlow Custom Data Sources

Like MPLS traffic, we can now define the subsets of traffic within the NetFlow data source that we wish to monitor. The default NDE data source, created when a device is added to the NAM NetFlow table, is an aggregate of the data on all NetFlow enabled interfaces of a device. To allow the user to focus in on a particular flow (one or more interfaces), a custom NDE data source can be created which extracts out the desired flows and treats this subset as a distinct data source in which NAM analysis and reporting can be performed against. Although this is a useful feature, the user should take care when both adding devices and creating custom NDE data sources so as not to over burden the NAM. Remember, a well thought out plan will only have the needed data forwarded to the NAM and enabled for only the necessary monitoring activities.

To create a custom NDE data source, first select the **Setup > Data Sources > NetFlow > Custom Data Sources** task. A table will be displayed showing all the default NDE data sources (aggregate of all NetFlow enabled interfaces from a device) and any previously created custom data sources. All custom data sources for a device will be listed under the default data source for the device. Click the **Create** button to configure a new custom data source as described next.

Basic NAM Configuration

NetFlow Custom Data Sources, continue ...

Same for NAM-1, NAM-2, and NM-NAM

3 Step wizard – select device, name data source, select interfaces, and verify.

Only Add NetFlow enabled interfaces!

Use the listening mode to determine which interfaces are NetFlow enabled

All device interfaces, not just NetFlow enabled interfaces, are listed (retrieved via SNMP)

NetFlow Data Sources - Device Selection

Select Device

Device: 192.168.79.110

Data Source Name: To WAN

< Back Next > Finish

NetFlow Data Sources - Select Interfaces

Select Interfaces

Data Flow: ☐ Input ☒ Output ☐ Both

Available Interfaces

- Special (0)
- Fa2/0 (1)
- Se3/0 (2)
- Se3/1 (3)
- Se3/2 (4)
- Se3/3 (5)
- Fa4/0 (6)
- Nu0 (7)
- Lo0 (8)
- Se3/0.1 (9)
- Se3/0.2 (10)
- Se3/0.3 (11)

Selected Interfaces

- Se3/0.1 (9) (Output)

Add Remove Remove All

< Back Next > Finish Cancel

NetFlow Data Sources - Summary

Data Source Summary

Device:	192.168.79.110
Name:	NDE-To WAN
Selected Interfaces:	Se3/0.1 (9) (Output)

< Back Next > Finish Cancel

Creating a NetFlow Custom Data Source

The creation of a custom NDE data source uses a three part wizard.

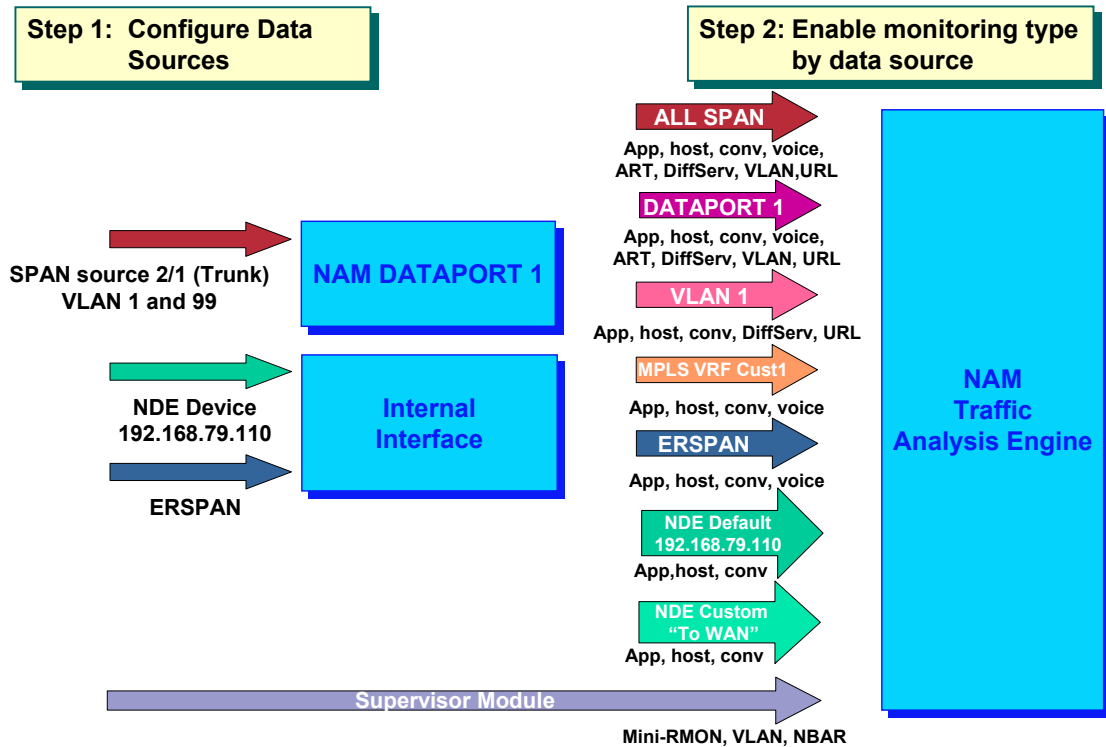
After selecting the **Create** button from the table displayed by selecting **Setup > Data Sources > NetFlow > Custom Data Sources**, the first step of the wizard is used to name the custom data source and to select the source NDE device. The pull down list of devices only includes devices that were added to the NAM NetFlow table. A default name will be constructed if the name field is left blank. It is always good practice to name managed components with a descriptive name to assist analysis when viewing the item on reports. Click the **Next** button to move to the second step of the wizard.

The second step of the wizard is used to select the subset of all NetFlow traffic from the device. This is done by selecting the desired NetFlow enabled interface(s). *The dialog lists all device interfaces and not just the NetFlow enabled ones, so select the interface accordingly.* As describe previously, the NetFlow Listening Mode task is used to determine all devices that are sending NetFlow traffic to the NAM. By looking at the listening mode details of a particular device, the user can determine the NetFlow enabled interfaces (and traffic direction) that are being reported by this flow. Use this information to properly select the interfaces and traffic directions to use in the custom data source.

The final step of the wizard is used to verify the configured custom data source. Select **Finish** to enable the custom data source.

Basic NAM-1/2 Configuration

Step 2: Enabling Core Monitoring



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-71

Enabling Data Collection (NAM-1/2)

After you have configured the data sources (SPAN / VACL / NetFlow), you are ready to begin configuring data collection. Enabling data collection entails configuring the NAM to collect specific types of data, listed below, from the various data sources.

- **ALLSPAN** – Monitors all traffic forwarded to the NAM-1/2 by means of spanning sessions and VACL traffic
- **DATAPORT X** – Monitors all traffic forwarded to an individual NAM-2 data port by means of Spanning sessions and VACL traffic (NAM-2 option only)
- **VLAN X** – Monitors all traffic forwarded to the NAM-1/2 by means of spanning sessions and VACL traffic that has membership in the VLAN selected
- **ERSPAN** – Monitors all traffic received via ERSPAN
- **MPLS Tag X** – Monitors all traffic forwarded to the NAM-1/2 by means of spanning sessions and VACL traffic that has membership in the MPLS traffic flow selected
- **NDE default** – Monitors all NetFlow traffic sent by a single NetFlow device
- **NDE Custom** – Monitors a subset of NetFlow traffic from a single device

Enabling data collection informs the NAM how to analyze the data, including what tables, graphs, and charts will be generated, and how many entries each report will contain.

The figure above shows an example of the data streams available for analysis on a NAM-1/2. The “stream” forwarded to the NAM-1/2 data port is a single port albeit a trunk. Possible data streams to enable analysis for include **All SPAN** which is an aggregate of all traffic sent to the NAMs data ports, **Dataport X** which is an aggregate of all traffic sent to the data port, **VLAN 1** which is a subset of all traffic sent to the NAM, **MPLS VRF:cust1** which is a subset of all traffic sent to the NAM, **ERSPAN** which is an aggregate of all ERSPAN traffic sent to the NAM, **NDE Default for 192.168.79.100** which is an aggregate of all NetFlow packets from that device, **Custom NDE “TO WAN”** which is a subset of the NDE packets from 192.168.79.100, and finally **Supervisor** which includes mini-RMON, VLAN, and NBAR statistics from the host switch.

Enabling Core Monitoring (NAM-1/2)

Configuring Monitoring Parameters

This table lists all the available monitoring options. It enables you to choose how you want the data to be analyzed.

This option enables you to define the data source that will populate the monitoring functions you choose.

The Monitoring Function options enable you to define the monitoring and reports that will be generated for each data source in the pull-down menu (*Options change depending on source*).

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	100
<input type="checkbox"/> Host Statistics (MAC layer)	Not applicable
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	500
<input type="checkbox"/> Conversation Statistics (MAC layer)	Not applicable
<input checked="" type="checkbox"/> VLAN Traffic Statistics	Not applicable
<input type="checkbox"/> VLAN Priority (CoS) Statistics	Not applicable
<input type="checkbox"/> Network-to-MAC Address Correlation	Not applicable

Configuring Monitoring Parameters

Step one of the basic NAM configuration simply passes data to the NAM. Now you must tell the NAM which statistics to collect on the traffic. The configuration of various monitoring functions for individual data sources is done from the dialogs found under the **Setup > Monitor** menu. To enable data collection and view results under the Monitor tab, you must do the following:

- Choose **Core Monitoring** from the menu on the left corner of the screen.
- Choose your data source from the pull-down list at the top of the Monitoring Functions box. The next few pages cover the available data source options and how to make effective use of them
- Choose the types of statistics that you wish to collect on the data source and set the configuration options found in the menu on the right side.

By executing each of these steps, you will configure the NAM to collect and analyze data from your data sources and report the statistics in the tables, graphs, and charts found under the **Monitor** tab.

Note(s):

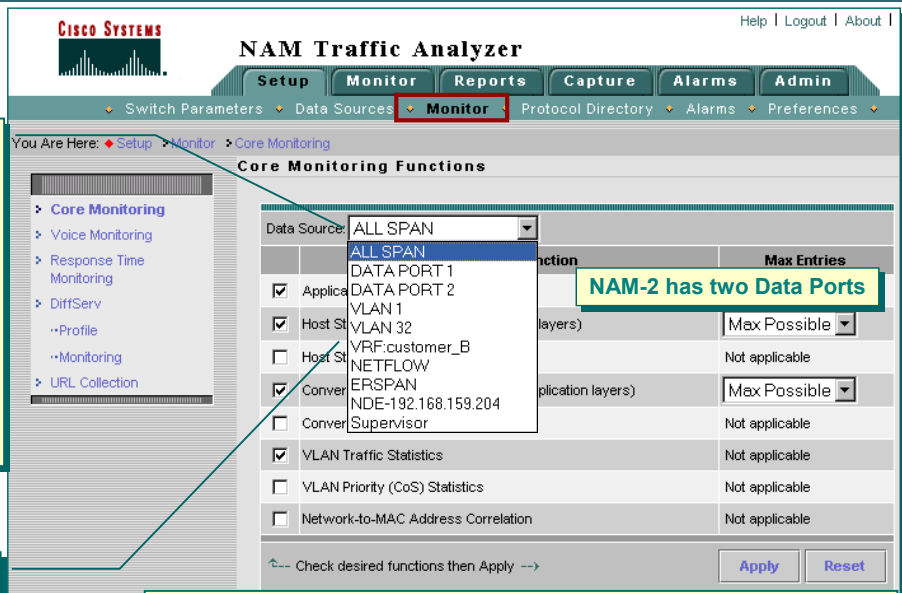
- *On the NAM-1/2, when changing spanned data sources, the statistics enabled are not cleared. Therefore, remember to clear out data collection configurations when changing spanning; otherwise, it will still be selectable as a data source for the various reports, but no data will exist.*

Enabling Core Monitoring (NAM-1/2)

Selecting Data Sources to Configure

- The ALLSPAN data source aggregates all of the *Spanned* and VACL statistics into a single data source.
- DATAPORT provides statistics for all traffic forwarded to the specified data port.
- VLAN specific statistics provided by individual VLAN data source

The NAM presents all known VLANs on the switch in the pull-down menu



- For better overall system performance, enable only the collections you want to monitor.
- Disable all functions for the collections you want to turn off. If you turn off collections that have reports running on them, the collections will automatically be turned on.

Selecting NAM-1/2 Data Sources to Configure

For the Catalyst 6500 Series NAM 1/2, the following data sources are available for configuration:

- ALL SPAN - ALLSPAN is a pull-down list option that enables you to aggregate all the VLANs that are part of your SPAN / VACL data source. The pull-down lists just the VLANs that it discovers as part of your SPAN / VACL source. Applying data collection to the ALLSPAN option will aggregate all VLAN data into a single data source—ALLSPAN. Configuring ALLSPAN alone for data collection will not provides statistics on a per-VLAN basis.
- VLANs - If you want to view statistics on a per-VLAN basis, you must choose each VLAN, one by one, and check each data collection function you want for each VLAN.
- MPLS - If you want to view statistics on a per-MPLS basis, you must choose each MPLS, one by one, and check each data collection function you want for each MPLS.
- ERSPAN
- NETFLOW
- NDE – Configure per NetFlow reporting device
- Supervisor – Mini-RMON and VLAN statistics sent directly to the NAM for reporting

Note(s):

- *Spanned data sources are enabled by VLAN even if what was spanned was a single port. In order to view traffic for that port, determine which VLAN that port is a member of and enable monitoring for that VLAN.*

Enabling Core Monitoring (NAM-1/2)

Selecting Statistics to Collect

Core Monitoring Functions

Data Source: ALL SPAN

Monitoring Function	
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	Max Possible
<input checked="" type="checkbox"/> Host Statistics (MAC layer)	Not applicable
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	Max Possible
<input checked="" type="checkbox"/> Conversation Statistics (MAC layer)	Not applicable
<input checked="" type="checkbox"/> VLAN Traffic Statistics	Not applicable
<input checked="" type="checkbox"/> VLAN Priority (CoS) Statistics (Class of Service)	Not applicable
<input checked="" type="checkbox"/> Network-to-MAC Address Correlation	Not applicable

Check desired functions

Apply Res

If you want individual VLAN monitoring, you must configure each VLAN data source for each monitoring function you want.

These options enable you to define how many entries the NAM will include in the reporting. These options affect NAM resource consumption.

• Enable RMON and VLAN statistics to be collected and reported on per data source

• ALL SPAN, Data Port, ERSPAN, and VLAN data sources all have the same enabling functions

Selecting Statistics to Collect

You can enable or disable individual core data collections on each available data source. The following core collections are available on the ALL SPAN, DATA PORTS, and VLAN data sources:

- Application Statistics--Enables the monitoring of application protocols observed on the data source.
- Host Statistics (Network and Application layers)--Enables the monitoring of network-layer host activity.
- Host Statistics (MAC layer)--Enables the monitoring of MAC-layer hosts activity. Also enables monitoring of broadcast and multicast counts for host detail screens.
- Conversation Statistics (Network and Application layers)--Enables the monitoring of pairs of network-layer hosts that are exchanging packets.
- Conversation Statistics (MAC layer)--Enables the monitoring of pairs of MAC-layer hosts that are exchanging packets.
- VLAN Traffic Statistics--Enables the monitoring of traffic distribution on different VLANs for the data source.
- VLAN Priority (CoS (Class of Service)) Statistics--Enables the monitoring of traffic distribution using different values of the 802.1p priority field.
- Network-to-MAC Address Correlation--Enables the monitoring of MAC-level statistics, which are shown in host detail windows. Without this collection, a MAC station cannot be associated with a particular network host.

Enabling Core Monitoring (NAM-1/2)

Selecting Statistics to Collect, continue ...

The screenshot shows the 'Data Source' dropdown set to 'NETFLOW'. Below it is a table with two columns: 'Monitoring Function' and 'Max Entries'. Three rows are visible, each with a checked checkbox in the first column. The first row is 'Application Statistics' with 'Not applicable' in the second column. The second row is 'Host Statistics (Network & Application layers)' with '1000' in the second column. The third row is 'Conversation Statistics (Network & Application layers)' with '5000' in the second column. At the bottom, there is a button labeled 'Apply' and a button labeled 'Reset'.

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	1000
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	5000

- Enable application protocol, hosts, and conversation statistics for each NetFlow, NDE, and MPLS data source to be monitored
- VLAN and Address Correlation statistics not available on NetFlow and MPLS data sources

The screenshot shows the 'Data Source' dropdown set to 'Supervisor'. Below it is a table with two columns: 'Monitoring Function' and 'Max Entries'. Three rows are visible, each with a checked checkbox in the first column. The first row is 'Port Stats (Mini-Rmon)' with 'Not applicable' in the second column. The second row is 'Vlan Statistics' with 'Not applicable' in the second column. The third row is 'NBAR Statistics' with 'Not applicable' in the second column. At the bottom, there is a button labeled 'Apply' and a button labeled 'Reset'.

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Port Stats (Mini-Rmon)	Not applicable
<input checked="" type="checkbox"/> Vlan Statistics	Not applicable
<input checked="" type="checkbox"/> NBAR Statistics	Not applicable

Enabling collection of mini-RMON statistics

- If the **Supervisor** module is configured to collect these statistics, these options allow the NAM to gather and report on them
- Without these functions enabled, the statistics will not be available in the NAM for reporting

Selecting Statistics to Collect, continue ...

The NetFlow, MPLS, and Supervisor data sources have slightly different Core Monitoring functions that can be enabled.

NetFlow, MPLS, and the Supervisor data sources may have been previously configured to gather statistics. But in order to have the NAM gather these statistics and have them available for reporting, these functions must be enabled, as illustrated above.

The switch engine module (Supervisor) can have its statistics received by the NAM by enabling these checkboxes. You can select any combination of Port statistics, VLAN statistics, and NBAR statistics.

Enabling Core Monitoring (NAM-1/2) Example

Step 1: Create a SPAN session that uses the ports 1/1 and 1/2 as your SPAN source and view your configuration settings via the Active Sessions Menu.

You Are Here: Setup > SPAN Sources

Active SPAN Sessions

Type	Source	Dest. Port	Dest. Module	Direction	Status
port	1/1 1/2	5/1	5	Both	active

↑--Select a SPAN session then take an action-->

Create Edit Delete

Ports 1/1 and 1/2 are members of VLAN 904.

You Are Here: Setup > Monitor > Core Monitoring

Core Monitoring Functions

Data Source: VLAN 904

Monitoring Function	Max Entries
<input type="checkbox"/> Application (Application layers)	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	100
<input type="checkbox"/> Host Statistics (MAC layer)	Not applicable
<input type="checkbox"/> Conversation Statistics (MAC layer)	Not applicable
<input type="checkbox"/> VLAN Priority (CoS) Statistics	Not applicable
<input type="checkbox"/> Network-to-MAC Address Correlation	Not applicable

↑-- Check desired functions then Apply -->

Apply Reset

Step 3: View Network Host Statistics Report by choosing the VLAN you configured in Step 2.

Network Hosts

Per-Second Data: as of Wed May 15 08:36:40 2002

☒ Auto Refresh

Current Rates Top/Bottom Cumulative Data

Data Source: VLAN 904

	Address	Filter	Clear		Via	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	Non-unicast/s
1	192.168.79.2			0.90	0.79	79.62	939.03	0.00		
2	192.168.79.3			0.21	0.97	84.31	413.14	0.00		
3	192.168.79.5			0.76	0.76	211.21	211.72	0.00		
4	192.168.79.1			0.17	0.17	74.90	74.55	0.00		
5	192.168.79.10			0.66	0.76	910.90	40.55	0.00		
6	192.168.79.2			0.00	0.59	0.00	41.59	0.59		
7	192.168.79.3			0.00	0.59	0.00	41.59	0.59		
8	192.168.79.50			0.79	0.59	332.83	41.59	0.59		
9	192.168.79.50			0.00	0.59	0.00	41.17	0.59		
10	10.1.4.2			0.03	0.55	3.52	38.90	0.55		
11	10.1.4.3			0.00	0.55	0.00	38.90	0.55		
12	192.168.79.10			0.10	0.17	26.00	33.07	0.00		
13	192.168.79.10			0.10	0.10	23.62	24.55	0.00		
14	192.168.79.11			0.10	0.10	14.72	15.00	0.00		
15	192.168.79.11			0.00	0.03	0.00	11.83	0.03		

Lists all hosts in VLAN 904 on ports 1/1 and 1/2

Step 2: Configure monitoring using the VLAN that your SPAN source (ports 1/1 and 1/2) are a member of (VLAN 904) as your data source. Then choose Host Statistics to enable monitoring of host traffic.

Monitor Configuration Example

To clarify these points, let's look at an example. In the example illustrated above, we want to use port spanning to see who is generating network and application traffic on ports 1/1 and 1/2. To do this, do the following:

- Step 1: Create a SPAN session using ports 1/1 and 1/2 as the SPAN source. Use the *Active SPAN Sessions* window to ensure that the SPAN session is correctly configured.
- Step 2: Gather information from the switch itself to determine which VLANs the source SPAN ports belong to. (CiscoWorks Campus Manager can also provide this information) In this case, it is VLAN 904. From the *Setup > Monitor* menu, choose *Core Monitoring* to configure monitoring. From the menu Data Source pull-down list, notice that all the VLANs that the switch knows about will be presented. Choose only the VLAN that the ports belong to, VLAN 904. From here, choose *Host Statistics (Network and Application layers)*.
- Step 3: Then go to the *Monitor > Host Statistics* menu. This brings you to the Network and Application Layer Host report that you chose in Step 2. You should see from the Data Source pull-down list in the Monitor menu only the data sources this you have configured for Host Statistics, in this case VLAN 904. If more data source options appear than you have configured, then return to the *Setup > Monitor > Core Monitoring* submenu to review whether or not you want to continue collecting statistics for those additional data sources that were listed in the Monitor pull-down list.

You should remember two points here. First, *always* remember where your data is coming from: both the SPAN Source and the VLANs that your SPAN source belongs to. Second, remember to set up monitoring to match the VLANs that correspond with your SPAN source and then confine monitoring to the VLANs that match your SPAN source.

Note: In this instance, because the ports both belong to a single VLAN, the ALLSPAN data source could also have been used. Now you are ready to move on to configuring the NAM and the Traffic Analyzer software to monitor and generate reports.

Basic NM-NAM Configuration Overview of Steps

See earlier slides for
NetFlow setup

Step 1

- Configure CEF using Router CLI to forward interface packets to the NM-NAM internal interface

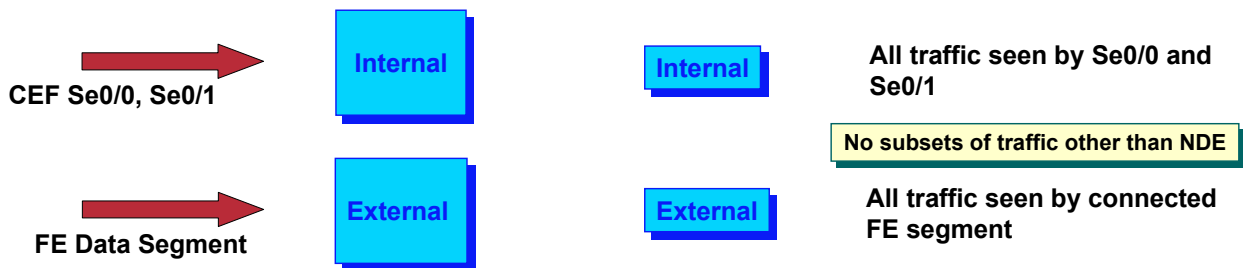
```
Router (config)# ip cef
Router (config)# interface type slot|wic-slot|port
Router (config-if)# analysis-module monitoring
```

Repeat steps 2 and 3 for each interface to monitor

Step 2

- Turn on types of monitoring (Application, host, conversation, ...) for data streams
 - Internal
 - External
 - ALL NDE Traffic from device
 - Subset of NDE traffic from a device

- Connect NM-NAM external interface to a Fast-Ethernet source



Basic NM-NAM Configuration Process

Like the NAM-1/2, the configuration of monitoring for the NM-NAM is also a two step process. First data must be sent to the NM-NAM for analysis, and secondly, various monitoring options must be enabled for each monitoring interface on the NM-NAM for analysis. Unlike the NAM-1/2, the NM-NAM does not break down the received traffic into subsets. Each NM-NAM interface simply analyzes the stream on it regardless of what it represents. The exception to this is the NDE traffic will actually be reported on as a separate data stream.

Data can be sent to the NM-NAM by:

- Using CEF to copy packets from a router interface to the internal NM-NAM interface
- Connecting the External NM-NAM interface to a FE source (HUB or SPAN port)

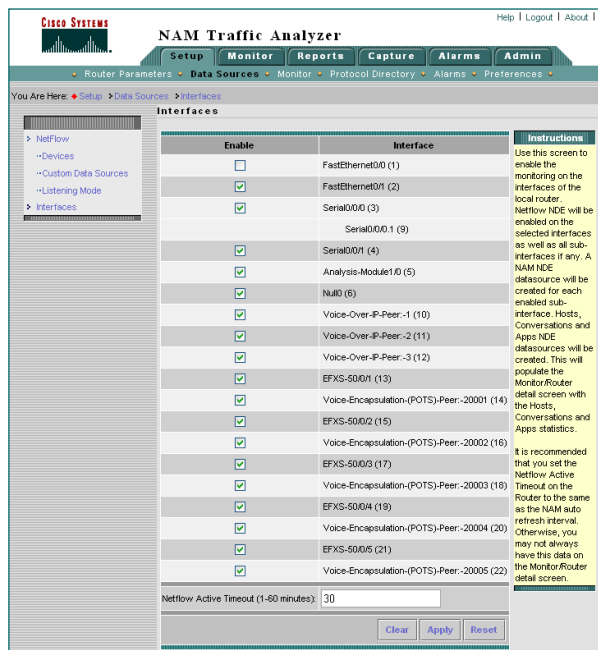
At this point the data is being sent to the NAM but not yet being analyzed. The second step is to turn on various monitoring options for the Internal and External interfaces, as well as the NDE default data stream – Monitors all NetFlow traffic sent by a single NetFlow device, and any NDE Custom data stream – Monitors a subset of NetFlow traffic from a single device.

Note: NDE traffic is sent to the NM-NAM interface configured as the Management port.

Earlier we discussed using NetFlow as a data source. NetFlow is also an applicable data source on the NM-NAM.

Basic NM-NAM Configuration

Host Interface



When local Interfaces are enabled to be monitored, the NM-NAM will automatically interact with the router to:

- Enable NetFlow Data Export (NDE) on the router Interfaces
- Set itself as the destination for NDE

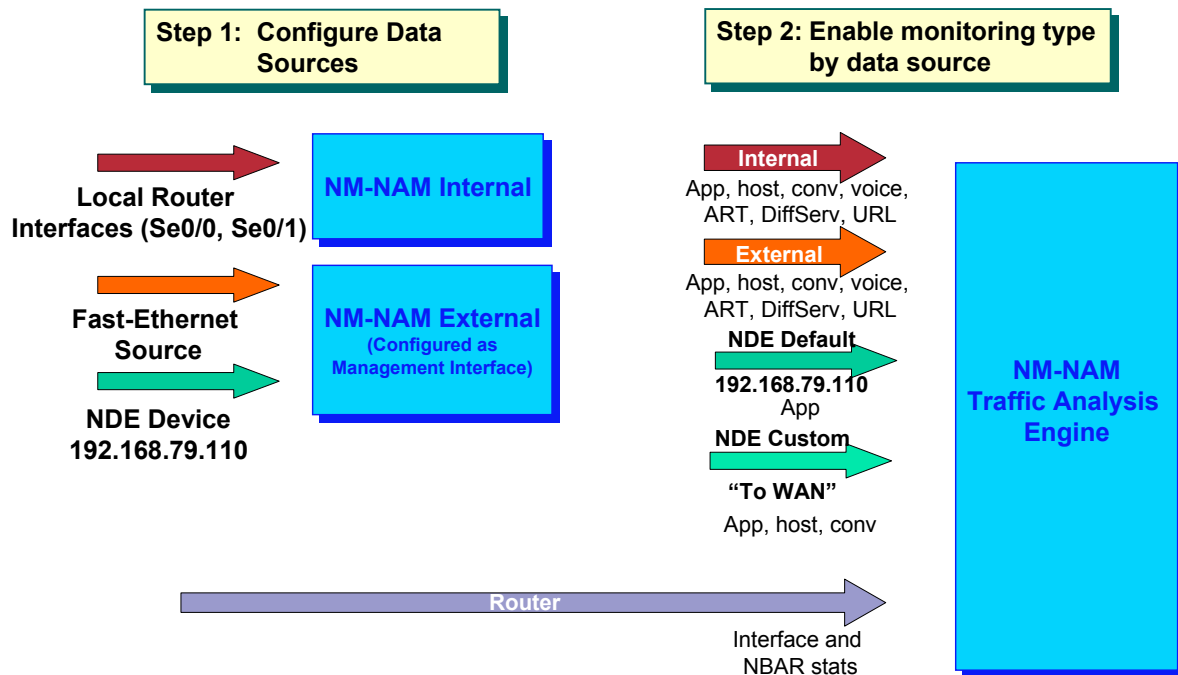
Provides App, Host, and Conv data with no further set-up

Host Interface

The NM-NAM will provide basic layer 2 statistics for each interface of the host device using MIB-II variables. To get further analysis of the traffic on any interface one could use CEF to forward the traffic to the NM-NAM or use the NM-NAM interfaces feature. When using this feature, **Setup > Data Sources > Interfaces**, the administrator is provided with a list of all interfaces discovered on the host device. By enabling desired interfaces, the NM-NAM enables NetFlow export on those interfaces and sets itself as the destination. As will be seen later on, the user can then see app, host, and conv statistics for each enabled interface using the **Monitor > Router > Interfaces** report.

Basic NM-NAM Configuration

Step 2: Enabling Core Monitoring



Enabling Data Collection (NM-NAM)

The NM-NAM differs from the NAM-1/2 in that NetFlow traffic is received on the NM-NAM interface configured as the management interface and there is no subset data streams other than the NDE traffic. So in the above example, traffic from interfaces Se0/0 and Se0/1 are being copied to the internal interface and the external interface is connected to a Fast Ethernet segment. The resulting data streams that must be enabled for analysis are Internal which is the aggregate of traffic on Se0/0 and Se0/1, External which is all traffic seen on the connected segment, NDE Default which is all NetFlow traffic from device 192.168.79.110, NDE Custom "To WAN" which is a subset of NDE traffic from 192.168.79.110, and Router which includes NBAR and MIB-II interface statistics.

Now let's look at how to enable some of these data streams for analysis.

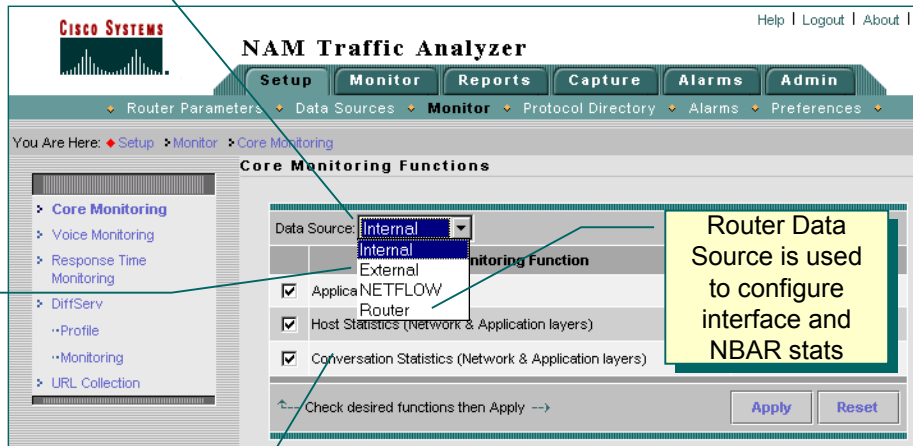
Enabling Core Monitoring (NM-NAM)

Selecting Data Sources to Configure

Internal data source includes all interfaces on the router configured to forward packets to the NM-NAM. Likewise, External includes all packets on the “wire” connected to the external NM-NAM interface

Data Source list includes default and custom NDE data sources.

The NM-NAM performs analysis on layers 3-7 on all packets on the NM-NAM interface. The data source is not broken down into individual streams like the VLANs on the NAM-1/2, hence there are fewer monitoring options



Router Data Source is used to configure interface and NBAR stats

Selecting NM-NAM Data Sources to Configure

Before looking at configuration examples, let's briefly look at the differences in the NM-NAM configuration. The basic configuration still applies – you must enable the type of analysis to perform on each data stream. What is different is that the NM-NAM is not VLAN centric like the NAM-1/2. In fact, when using the NM-NAM, you will not see any reference to a VLAN. Simply pick the data source and enable the desired analysis. There is no breaking down of the data sources into individual streams of data like interfaces. The exception to this is the NDE data sources which can be broken down by NDE devices.

Now let's take a look at enabling data collections on the NM-NAM.

Types of Statistics Collected

<input checked="" type="checkbox"/>	Application Statistics	Enables the monitoring of application protocols observed on the data source
<input checked="" type="checkbox"/>	Host Statistics (network and application layers)	Enables the monitoring of network-layer host activity
<input type="checkbox"/>	Conversation Statistics (network and application layers)	Enables the monitoring of pairs of network layer hosts that are exchanging packets
<input type="checkbox"/>	Host Statistics (MAC layer)	Enables the monitoring of MAC-layer hosts activity; also enables monitoring of broadcast and multicast counts for host detail screens
<input type="checkbox"/>	Conversation Statistics (MAC layer)	Enables the monitoring of pairs of MAC-layer hosts that are exchanging packets
<input checked="" type="checkbox"/>	VLAN Traffic Statistics	Enables the monitoring of traffic on different VLANs for the data source
<input type="checkbox"/>	VLAN Priority (CoS) Class of Service Statistics	Enables the monitoring of traffic using different values of the 802.1p priority field
<input checked="" type="checkbox"/>	Network-to-MAC Address Correlation	Enables the monitoring of MAC-level statistics that are shown in host detail windows; without this collection, a MAC station cannot be associated with a particular network host

NDE and NM-NAM data sources provide monitoring for these 3 groups of statistics

Enabling Core Monitoring

In the Core Monitoring menu, you are presented with all the monitoring and reporting options available to identify most of the network, application, and VLAN reports that are provided by RMON and SMON MIBs. To configure the NAM to collect and monitor any of these options for a given data source, first select the data source from the pull-down menu and then simply check the box to the left of the desired monitoring option. Core Monitoring options include:

Application statistics: This option enables monitoring and reporting by application protocol. This is useful for identifying which protocols are consuming the most bandwidth and enables proactive planning based on application usage patterns.

Host statistics (network and application layers): This option enables host monitoring and reporting by network address. This information is useful for identifying which stations, servers, and end users are generating the most traffic by network and application protocol.

Host statistics (MAC layer): This option enables host monitoring at the MAC layer, Layer 2. Not available for NM-NAM and NDE data sources.

Conversation statistics (network and application layer): This option provides monitoring by network layer host pairs. This is very useful to identify utilization patterns between clients and servers and can also be used to identify configuration errors for network devices and identify broadcast and multicast traffic by network address.

Conversation statistics (MAC layer): This option provides monitoring by MAC layer host pairs. This can often be useful in identifying configuration errors for networked devices, and it identifies broadcast and multicast traffic by MAC address. Not available for NM-NAM and NDE data sources.

VLAN traffic statistics: This option enables monitoring and reporting distribution by VLANs. This is useful for identifying resource usage patterns by VLANs. Available only for ALLSPAN and DATAPORT aggregation data sources. Not available for NM-NAM and NDE data sources.

VLAN priority: This option enables monitoring VLANs by the values set in the 802.1p priority fields. This can be used to validate class-of-service (CoS) configuration. Not available for NM-NAM and NDE data sources.

Network-to-MAC address correlation: This option enables monitoring MAC-layer statistics that populate the host detail views. This also provides network address-to-MAC address correlation. If you turn this off, the NAM will not associate MAC address with network layer host information. Not available for NM-NAM and NDE data sources.

Types of Statistics Collected

Application



Application Statistics

Enables the monitoring of application protocols observed on the data source

Choosing Application Statistics from the **Setup > Monitoring > Core Monitoring** menu enables the illustrated statistics by application protocol.

Selecting the Data Source to see Application Statistics for

Selecting a protocol from this report will provide a new report listing all hosts sending traffic using this protocol.

Current Rates for Application Statistics

Showing 1-10 of 33 records

#	Protocol	Packets/s	Bytes/s
1.	snmp	2.16	635.95
2.	smb	0.80	153.12
3.	icmp	1.42	149.51
4.	http	0.22	144.34
5.	cisco-net-mgmt	0.16	131.47
6.	igmp	1.51	124.04
7.	hsrp	1.44	100.87
8.	tcp-unknown	0.64	98.57
9.	sstp	1.00	72.00
10.	smb	0.19	52.69

Rows per page: 10 Go to page: 1 of 4

Select an item then take an action --> Details Capture Real-Time Report

Monitor > Apps

Core Monitoring: Application Statistics

The illustration provides an example of the reports you will see by enabling Application Statistics from the **Setup > Monitor > Core Monitoring** menu. The results of checking this box will be seen in many areas of the Monitoring section, but this sample shows information useful for identifying which protocols are consuming the most bandwidth and enables proactive planning based on application usage patterns.

Note: Selecting any application in this report will display a drill-down report showing all hosts using this application. More on this report and its options later in this chapter.

Types of Statistics Collected Hosts



Host Statistics (Network and Application layers)

Enables the monitoring of network layer host activity

Current Rates for Network & Application Layer Statistics

Current Rates TopN Chart Cumulative Data

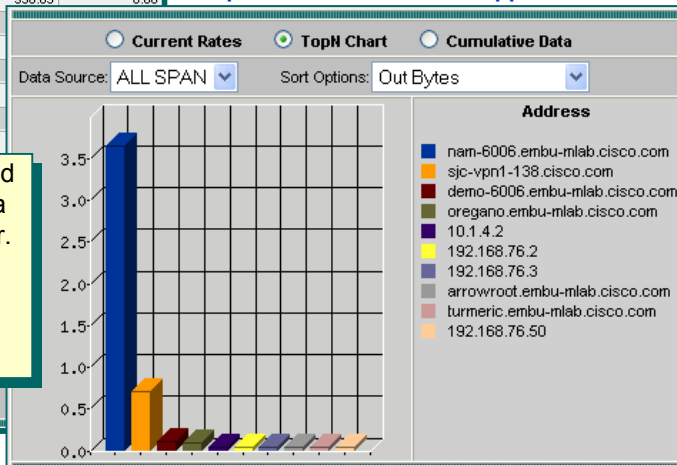
Data Source: ALL SPAN Address: Filter Clear

		Via	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	Non-Unicast/s
1.	nam-6006.embu-mlab.cisco.com	ip	0.90	0.79	76.62	938.03	0.00
2.	chicory.embu-mlab.cisco.com	ip	0.21	0.97	84.31		
3.	demo-6006.embu-mlab.cisco.com	ip	0.76	0.76	211.21		
4.	balsamic.embu-mlab.cisco.com	ip	0.17	0.17	74.90		
5.	sjc-vpn1-1145.cisco.com	ip	0.66	0.76	910.90		
6.	192.168.76.2	ip	0.00	0.59	0.00		
7.	192.168.76.3	ip	0.00	0.59	0.00		
8.	192.168.76.50	ip					
9.	arrowroot.embu-mlab.cisco.com						
10.	10.1.4.2						
11.	10.1.4.3						
12.	oregano.embu-mlab.cisco.com						
13.	anise.embu-mlab.cisco.com						
14.	rosemary.embu-mlab.cisco.com						
15.	192.168.76.11						

Go To Entry: of 26 Go

Choosing Hosts Statistics from the **Setup > Monitoring > Core Monitoring** menu enables the following statistics by network and application.

TopN Chart for Network & App Statistics



Note that only VLAN 904 and ALLSPAN appear as a data source option under Monitor. This is because we only configured these Data Sources for host statistics monitoring.

Monitor > Hosts > Network Hosts

Core Monitoring: Host Statistics

This illustration provides an example of the reports you will see if you choose *Network Hosts Statistics* from the **Setup > Monitor > Core Monitoring** menu. As you can see, the Host Statistics table provides you with the host names or network address of the hosts that it has discovered as well as statistics by network layer protocol and the number of bytes and packets for every host. If you choose MAC layer host statistics (NAM-1/2 only), you will be presented with the same tables and charts, but MAC addresses will be presented in lieu of network host names or network addresses. This information is useful for identifying which stations, servers, and end users are generating the most traffic by network and application protocol or by Layer 2 MAC address.

Note: Selecting any host in this report will display a drill-down report showing all application conversations this host is involved in. More on this report and its options later in this chapter.

Types of Statistics Collected

Conversations



Conversation Statistics (Network and Application layers)

Enables the monitoring of pairs of network layer hosts that are exchanging packets

- Choosing Conversation Statistics (Network and Application layers) from the **Setup > Monitoring > Core Monitoring** menu enables traffic rates per conversation.
- Choosing MAC layer conversation statistics will give you the same data but will show MAC addresses rather than network addresses and host names.

Cumulative Data for Network and Application conversation statistics

☒ Current Rates
 ☐ TopN Chart
 ☐ Cumulative Data

Data Source: ALL SPAN
 Address:
Filter
Clear

Showing 1-10 of 608 records

	#	Source	Via	Destination	Packets/s	Bytes/s
<input type="radio"/>	1.	192.168.76.232	ip	64.101.33.159	115.00	85112.00
<input type="radio"/>	2.	192.168.76.232	ip	64.101.33.144	58.00	41897.00
<input type="radio"/>	3.	192.168.76.196	ip	10.21.65.60	87.00	27447.00
<input type="radio"/>	4.	192.168.76.239	ip	10.21.65.60	83.00	27435.00
<input type="radio"/>	5.	192.168.76.226	ip	64.103.107.226	25.00	25085.00
<input type="radio"/>	6.	192.168.76.226	ip	10.21.65.60	92.00	24085.00
<input type="radio"/>	7.	192.168.76.233	ip	10.21.65.60	83.00	24021.00
<input type="radio"/>	8.	192.168.76.232	ip	64.101.33.154	36.00	16416.00
<input type="radio"/>	9.	192.168.76.235	ip	10.21.65.60	80.00	10665.00
<input type="radio"/>	10.	192.168.76.237	ip	10.21.65.60	69.00	8714.00

Rows per page: 10
Go to page: 1 of 61
Go

Select an item then take an action -->
Details
Capture
Real-Time
Report

Monitor > Conversations > Network Hosts

Core Monitoring: Conversation Statistics

This illustration provides an example of the reports you will see if you choose *Conversation Statistics (Network and Application Layers)* from the *Setup > Monitor > Core Monitoring* menu. Notice that this table shows you who is talking with whom. In this example, you can see which network devices are using multicast addresses as destinations. You can use this information to identify utilization patterns between clients and servers and also to identify configuration errors for network devices and identify broadcast and multicast traffic by network address.

Note: Selecting any host in this report will display a drill-down report showing all application conversations the selected host is involved in. More on this report and its options later in this chapter.

Types of Statistics Collected

VLAN Traffic

NAM-1/2
Only



VLAN Traffic Statistics

Enables the monitoring of traffic on different VLANs for the data source

Choosing VLAN Traffic Statistics from the **Setup > Monitoring > Core Monitoring** menu enables the statistics illustrated in the table and chart.

Current Rates for VLAN Traffic Statistics

Current Rates TopN Chart Cumulative Data

Data Source: ALL SPAN

Showing 1-3 of 3 records

#	VLAN ID	Packets/s	Bytes/s	Non-Unicast Pkts/s	Non-Unicast Bytes/s
1.	60	6.50	2084.85	1.37	115.13
2.	100	3.18	293.40	3.18	293.40
3.	130	1.72	125.97	1.72	125.97

Rows per page: 20 Go to page: 1 of 1 Go

Select an item then take an action --> Report

Monitor > VLAN > Traffic Statistics

TopN VLAN Traffic Statistics



Core Monitoring: VLAN Traffic Statistics

This illustration provides an example of the reports you will see if you choose the *VLAN Traffic Statistics* option for the ALLSPAN, DATAPORT 1, and/or DATAPORT2 data sources from the *Setup > Monitor > Core Monitoring* menu. These reports provide traffic distribution statistics by VLAN number and can be useful for identifying resource usage patterns by VLAN ID.

Note: VLAN statistics will be provided only for VLANs present in the SPAN source unless the data source selected is Supervisor.

Types of Statistics Collected

VLAN Priority

NAM-1/2
Only



VLAN Priority (CoS) Statistics

Enables the monitoring of traffic using different values of the 802.1p priority field

Current Rates for VLAN Priority Statistics

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data			
Data Source: ALL SPAN			
	Priority	Packets/s	Bytes/s
1.	0	14.70	3579.31
2.	3	0.16	11.11

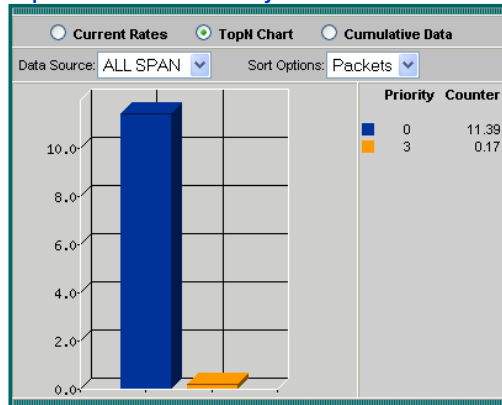
Monitor > VLAN > Priority (COS) Statistics

Cumulative Data for VLAN Priority Statistics

<input type="radio"/> Current Rates <input type="radio"/> TopN Chart <input checked="" type="radio"/> Cumulative Data			
Data Source: ALL SPAN			
	Priority	Packets	Bytes
1.	0	11568213	1154551508
2.	3	155751	10526050
3.	5	119	25942
<input type="button" value="Refresh"/>			

Choosing VLAN Priority Statistics from the **Setup > Monitoring > Core Monitoring** menu enables, as an example, the statistics by VLAN priorities.

TopN Chart for VLAN Priority Statistics



Core Monitoring: VLAN Priority Statistics

This illustration shows the reports you will see if you choose VLAN Priority Statistics from the **Setup > Monitor > Core Monitoring** menu. These reports provide statistics by aggregating traffic by the value in the 802.1p priority field. This information can be very useful for verifying CoS (configurations and identifying possible configuration problems).

Types of Statistics Collected (NAM-1/2)

Supervisor Data Source

Setup > Monitor > Core Monitoring

Data Source: Supervisor	
Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Port Stats (Mini-Rmon)	Not applicable
<input checked="" type="checkbox"/> Vlan Statistics	Not applicable
<input checked="" type="checkbox"/> NBAR Statistics	Not applicable
Check desired functions then Apply -->	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Enable statistics collection from Supervisor

Monitor > VLAN > Traffic Statistics

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data					
Data Source: Supervisor					
Showing 1-2 of 2 records					
#	VLAN ID	Packets/s	Bytes/s	Non-Unicast Pkts/s	Non-Unicast Bytes/s
<input type="radio"/> 1	2	24.93	45%	16,196.27	0.00
<input type="radio"/> 2	100	29.87	55%	3,747.25	17.02
Rows per page: 50 Units: Bytes/s Go to page: 1 of 1 <input type="button" value="Go"/> <input type="button" value="Report"/>					

Current statistics for all VLANs configured on Switch

Core Monitoring: Supervisor Data Source

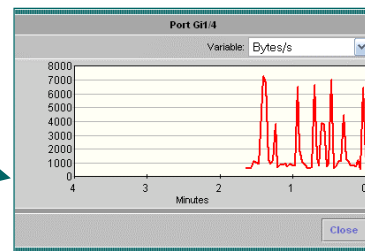
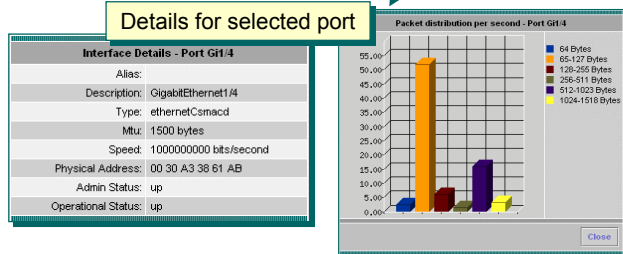
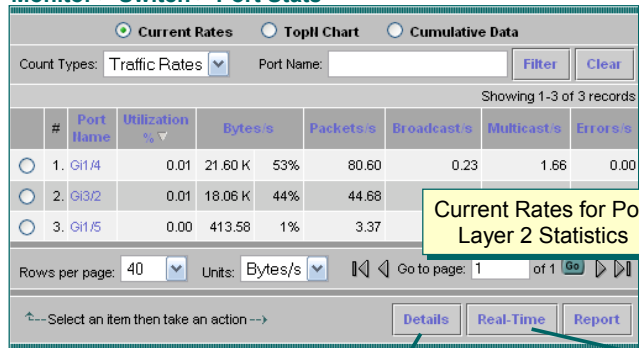
One of the data sources to be configured on the NAM-1/2 is called **Supervisor**. This data stream is the interface between the host switch and the Catalyst 6500 Series and Cisco 7600 Series NAM. This stream provides the NAM with mini-RMON and Supervisor VLAN information from the host switch. (NBAR statistics may not be implement on all switches.)

This illustration shows the real-time monitoring reports you would see if you choose *VLAN Statistics* from the **Setup > Monitor > Core Monitoring** menu with **Supervisor** as the data source.

Types of Statistics Collected (NAM-1/2)

Supervisor Data Source – Port Stats

Monitor > Switch > Port Stats



Core Monitoring: Supervisor Data Source – Port Stats

On the NAM-1/2 the mini-RMON statistics pulled from the host switch provide utilization and error statistics for each active port. Selecting a port and clicking **Details** provides information about the selected port and also presents a packet size distribution

Types of Statistics Collected (NM-NAM)

Router Data Source

Setup > Monitor > Core Monitoring

Data Source: Router	
Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Interface Statistics	Not applicable
<input checked="" type="checkbox"/> NBAR Statistics	Not applicable
↑... Check desired functions then Apply →	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Enable statistics collection for host Router Interfaces

Monitor > Router > NBAR

Current Rates | TopN Chart | Cumulative Data

Protocol: Filter Clear

Showing 1-6 of 6 records

#	Protocol	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Bit Rate/s	Out Bit Rate/s
1	snmp	0.72	68%	0.73	203.92	189.82	1.00
2	icmp	0.19	18%	0.21	18.44	20.04	0.00
3	unknown	0.14	13%	0.03	34.12	2.21	0.00
4	exchange	0.01	1%	0.02	0.53	0.94	0.00
5	rsvp	0.01	1%	0.00	2.36	0.00	0.00
6	netbios	0.00	<1%	0.00	0.00	0.33	0.00

Rows per page: 10 Units: Bytes/s/s Go to page: 1 of 1 Real-Time

Current rates for NBAR discovered protocols for selected interface

Core Monitoring: Router Data Source

One of the data sources to be configured on the NM-NAM is called **Router**. This data stream is the interface between the host router and the NM-NAM. This stream provides the NM-NAM with MIB-II interface statistics and NBAR information from the host router. This illustration shows the reports you will see if you choose **NBAR Statistics** from the **Setup > Monitor > Core Monitoring** menu with **Router** as the data source.

Types of Statistics Collected (NM-NAM)

Router Data Source – Interface Stats

Monitor > Router > Interface Stats

Current Rates TopII Chart Cumulative Data

Filter: Filter Clear

Showing 1-4 of 4 interfaces

#	Interface	In % Utilization	Out % Utilization	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Non-Unicast/s	Out Non-Unicast/s	In Discards/s	Out Discards/s	In Errors/s	Out Errors/s
1	Se0/0/0	100.00	100.00	100.82	101.38	30,206.35	48%	32,123.05	0.00	0.00	0.00	0.00	0.00
2	Se0/0/0.1	100.00	100.00	100.72	101.28	30,204.65	48%	32,121.75	0.00	0.00	0.00	0.00	0.00
3	An1/0	0.02	0.28	4.02	109.45	2,764.15	4%	35,292.85	0.02	0.12	0.00	0.00	0.00
4	Fa0/0	0.00	0.00	0.60	0.62	138.47	<1%	140.47	0.07	0.13	0.00	0.00	0.00

Rows per page: 15 Units: Bytes/s Go to page: 1 of 1

Select an item then take an action --> Details Real-Time Report

Current Rates
for Router
Interfaces

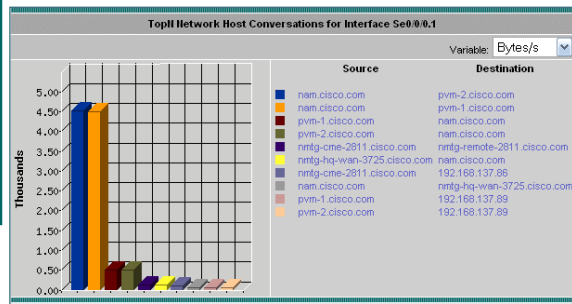
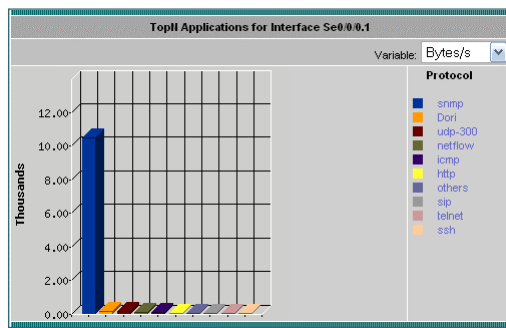
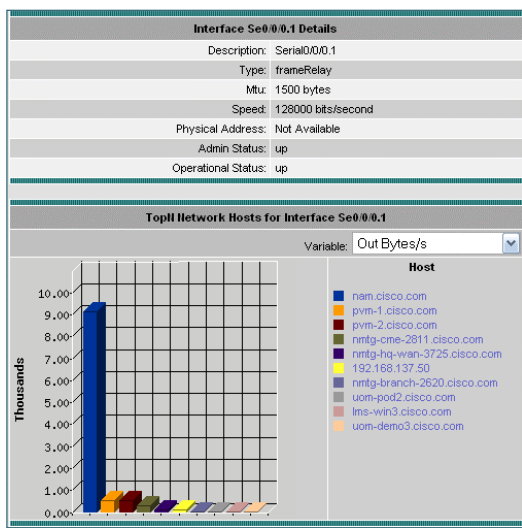
Select interface
and click Details
for App, Host,
and Conv data

Core Monitoring: Router Data Source – Interface Stats

The other available report from the **Router** data source is Interface Statistics. This gives you the basic layer 2 statistics for each interface on the host device. To see more detailed (enabled using **Setup > Data Sources > Interfaces**) select an interface and click **Details**.

Types of Statistics Collected (NM-NAM)

Router Data Source – Interface Stats Details



Core Monitoring: Router Data Source – Interface Stats Details

Is so enabled, you can see application, host, and conversation detail for the selected interface from the **Monitor > Router Interface > Stats** report.

Enabling Traffic Monitoring (NAM-1/2)

MPLS – Enable Monitoring

Setup > Monitor > Core Monitoring

Data Source: VRF:customer_B

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	100
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	500

←-- Check desired functions then Apply -->

Apply Reset

Enable application protocol, host, and conversation statistics for each MPLS data source to be monitored

View traffic statistics (packets, bytes) by MPLS Data Source

MPLS traffic must be present in the SPAN source

Monitor > MPLS > VRF Statistics

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Showing 1-1 of 1 records

#	VRF Name	In Pkts/s	In Bytes/s	Out Pkts/s	Out Bytes/s
1.	customer_B	4,256.33	100%	289,430.67	0.00

Rows per page: 15 Units: Bytes/s Go to page: 1 of 1

←--Select an item then take an action--> Report

MPLS Enable Monitoring

Earlier, we discussed using the **Setup > Data Sources > MPLS Data Sources > L3 VRF** task to set up MPLS traffic streams as subset data sources to be monitored. These data sources can be enabled for monitoring in the same way as all other data sources.

The NAM can analyze applications, hosts, and conversations and basic in/out statistics for each configured MPLS data source using the **Monitor > MPLS > VRF Statistics** task. (Basic statistics are also available for VC and label flows.)

Note: The NAM analyzes the MPLS traffic based on the tag inside the data packet. When NAM encounters stacked MPLS tags, the relevant inner-most tag is used for monitoring

Enabling Traffic Monitoring (NAM-1/2)

MPLS – RMON-2 Stats

Apps, Hosts, and Conv stats available for MPLS data sources just like ALL SPAN and VLANs, simply select MPLS from Data Source

You Are Here: [Monitor](#) > [Apps](#) > [Individual Applications](#)

Applications

Per-Second Data: as of Wed 12 Jul 2006, 19:31:07 UTC

☐ Auto Refresh

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source: [VRF:customer_B](#)

Showing 1-1 of 1 records

#	Protocol	Packets/s	Bytes/s	
1.	http	30,750.07	13,789,046.20	100%

Rows per page: [15](#) Units: [Bytes/s](#) Go to page: [1](#) of 1

↑...Select an item then take an action-->

Hosts using w-ether2.ip.tcp.http

Host	In Pkts	Out Pkts	In Bytes	Out Bytes
201.0.4.2	108,754,796	108,754,751	85,788,798,525	11,745,511,462
201.0.6.2	108,754,751	108,754,796	11,745,511,462	85,788,798,525

MPLS Enable Monitoring – RMON2 Stats

Since the MPLS data source is treated just like an NDE or VLAN data source, you are able to get basic RMON2 statistics for them (application, host, and conversation).

Enabling Traffic Monitoring Voice

Setup > Monitor > Voice Monitoring

	SCCP	H.323	MGCP	SIP
Monitoring Enabled:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number of phone table rows (10-1000):	300	200	200	200
Number of call table rows (10-1000):	300	200	200	200
Number of top packet jitter rows (1-20):	20	5	5	5
Number of top packet loss rows (1-20):	20	5	5	5
Debug:	<input type="checkbox"/>			
<div>Apply Reset</div>				

If you enable voice monitoring, the Traffic Analyzer software generates the Aggregate Statistics table as well as the detailed reports illustrated on the next page.

Enabling Voice Monitoring

Performance monitoring of voice applications is critical because voice traffic is much more sensitive to fluctuations in network performance than data. Packet loss and jitter are two very important indicators of call quality. The NAM can monitor voice-over-IP (VoIP) calls by collecting data from a variety of sources, including the Cisco Call Managers. It can also monitor VoIP performance by collecting SCCP, H.323, MGCP, or SIP packets between IP phones and the Cisco Call Manager that are generated during call setup and tear-down, giving you visibility into Cisco Call Manager and network performance (packet loss and jitter statistics). In addition, the NAM can monitor Real-Time Control Protocol (RTCP) to provide real-time reporting on call statistics.

Enabling voice monitoring is also a straightforward process. From the **Setup > Monitor** window, choose Voice Monitoring from the list in the left corner. The Voice Monitor Setup window allows you to turn on voice monitoring by protocol, either SCCP, H.323, MGCP, SIP or all four of them. You also have the option of defining how many voice call packet loss and jitter entries the NAM will track before overwriting the oldest entries with newer entries. The advantage to customizing these parameters is that it enables you to influence the amount of resources dedicated to this table. For example, more rows means that more memory in the NAM is allocated to the table. Adjusting your table size is one of the configuration parameters you will want to consider when you evaluate your monitoring needs against the resource utilization and performance of your NAM. To view the results of your configuration, choose **Monitor > Voice > Voice Overview** and drill down to the detail screen by choosing the protocol you want to view and clicking the Details button.

Enabling Traffic Monitoring

Example: Voice Overview

Monitor > Voice/Video > Voice Overview

Aggregate Statistics					
Protocol	Calls Monitored	Avg Pkt Loss (%)	Avg Jitter (ms)	Worst Pkt Loss (%)	Worst Jitter (ms)
<input checked="" type="radio"/> SCCP	3 K	0.00	0	0.00	0
<input type="radio"/> H.323	10	-	-	-	-
<input type="radio"/> MGCP	0	-	-	-	-
<input type="radio"/> SIP	0	-	-	-	-
Select a protocol then take an action -->					

Aggregate Statistics for Voice Calls

Detailed Reports for SCCP Packet Loss Statistics

Packet Loss - Worst Quality SCCP Calls								
Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter
<input type="radio"/> 1005	1001	-	-	Thu 20 Jul 2006, 12:03:20 PDT	192.168.137.60	192.168.137.62	0.00	0
<input type="radio"/> 1005	1001	-	-	Thu 20 Jul 2006, 09:15:14 PDT	192.168.137.60	192.168.137.62	0.00	0
Select an item then take an action -->								

Details for selected call

Jitter - Worst Quality SCCP Calls								
Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter
<input type="radio"/> 1005	1001	-	-	Thu 20 Jul 2006, 12:03:20 PDT	192.168.137.60	192.168.137.62	0.00	0
<input type="radio"/> 1005	1001	-	-	Thu 20 Jul 2006, 09:15:14 PDT	192.168.137.60	192.168.137.62	0.00	0
Select an item then take an action -->								

Voice Overview

Use the **Monitor > Voice/Video > Voice Overview** report to see packet loss and jitter statistics gathered for each enabled protocol. Selecting a protocol and clicking the **Details** button will display two tables showing the top 10 worst calls for both Packet Loss and jitter. Selecting one of these call and clicking **Details** presents detailed statistics for the individual call.

Enabling Traffic Monitoring

RTP Stream Monitoring

Setup > Monitor > RTP Stream Monitoring

NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Switch Parameters Data Sources Monitor Protocol Directory Alarms Preferences

You Are Here: Setup > Monitor > RTP Stream Monitoring

Stream Monitor Setup

Monitoring Enabled: ☒

Max Source Destination Entries: (1-100): 30

Apply Reset

Filter Table

Src Address	Src Mask	Dst Address	Dst Mask
0.0.0.0	0.0.0.0	172.20.0.0	255.255.0.0

← Check desired functions then Apply → Create Edit Delete

New Filter

Source Address: 192.168.0.0

Source Mask: 255.255.0.0

Destination Address: 0.0.0.0

Destination Mask: 0.0.0.0

OK Reset Cancel

- Monitor RTP streams
- View real-time video packet loss statistics
- Apply src/dest address filters to monitor key RTP streams of interest
- Obtain key data on RTP packet count, packet loss, and packet loss rate
- Set alarm thresholds on packet loss variables
- View RTP packet loss events as syslogs

RTP Stream Monitoring

You can monitor RTP video streams for packet loss statistics. To enable this feature, select **Setup > Monitor > RTP Stream Monitoring**.

Use filters (source and destination addresses) to monitor only RTP streams that are of interest.

Enabling Traffic Monitoring

Example: RTP Stream Monitoring

The screenshot shows the NAM Traffic Analyzer interface. The top navigation bar includes tabs for Setup, Monitor, Reports, Capture, Alarms, and Admin. The 'Monitor' tab is active, and the 'Voice/Video' section is selected. The 'RTP Stream Traffic' view is displayed, showing a table of RTP streams. The table has columns for #, Source Address, Source Port, Destination Address, Destination Port, RTP Payload Type, SSRC Value, and Packet Loss Rate 10⁻⁶. Two records are shown: Record 1 with Source Address 172.20.104.34, Source Port 23682, Destination Address 172.20.104.80, Destination Port 26010, RTP Payload Type PCMU, SSRC Value 343262100, and Packet Loss Rate 430; Record 2 with Source Address 172.20.104.80, Source Port 26010, Destination Address 172.20.104.34, Destination Port 23682, RTP Payload Type PCMU, SSRC Value 3421225620, and Packet Loss Rate 0. A 'Details' button is highlighted in the bottom right corner of the table.

RTP Packet Loss:

- Number of packets expected vs. Number of packets received

RTP Packet Loss Rate:

- $\frac{\text{Number of packet lost} + \text{number of packets received}}{\text{number of packets received}} \times 1,000,000$

Selected stream details

The 'Video Stream Details' dialog box displays the following information:

- Source Address: 172.20.104.34
- Source Port: 23682
- Destination Address: 172.20.104.80
- Destination Port: 26010
- Payload Type: PCMU
- SSRC: 343262100
- RTP Packet Count: 3137199
- RTP Packet Loss: 1356
- RTP Packet Loss Rate 10⁻⁶: 432
- Start Time: Mon 28 Nov 2005, 17:33:42 PST
- Last Timestamp: 859457856
- Last Sequence: 10964

A 'Close' button is located at the bottom right of the dialog box.

RTP Stream Monitoring Example

Use the **Monitor > Voice/Video > RTP Stream Traffic** to see packet loss statistics for the filters created. Packet loss is determined based on the number of packets expected (based on sequence numbers) versus the number of packets received.

Enabling Traffic Monitoring Response Time

Setup > Monitor > Response Time Monitoring

DataSource	
<input type="checkbox"/>	ALL SPAN
<input type="checkbox"/>	DATA PORT 1
<input type="checkbox"/>	DATA PORT 2
<input type="checkbox"/>	VLAN 1
<input type="checkbox"/>	VLAN 2
<input type="checkbox"/>	VLAN 100
<input type="checkbox"/>	VLAN 111

Select a control row then take an action -->

NAM-1/2

The first screen lists the data sources currently enabled for Response Time Monitoring data source.

DataSource	
<input type="checkbox"/>	External
<input checked="" type="checkbox"/>	Internal

Select a control row then take an action -->

NM-NAM

Enable Response Time Monitoring for available data streams by configuring response buckets.

Response Time Collection Configuration	
Datasource	VLAN 100
Report Interval (sec)	1800
RspTime1 (msec)	5
RspTime2 (msec)	15
RspTime3 (msec)	50
RspTime4 (msec)	100
RspTime5 (msec)	200
RspTime6 (msec)	500
RspTimeMax (msec)	3000
Max Entries in Tables	500

Select data source and configure timing buckets

Enabling Response Time Monitoring

Response time measurements can be a very useful indicator of server or network performance. You can use this monitoring function to warn you when a server or the network performance degrades. It works by collecting statistics based on unique values (TCP sequence and acknowledgement numbers) in the packets of conversations it observes in your data source. It then calculates the amount of time it took between a request and the acknowledgement of the request. It is absolutely critical to identify the best location for the NAM for accurate response-time reporting; otherwise your response-time numbers may not reflect the response-times you think they do. Let's review NAM placement for response time reporting: If you want to gather statistics about how long it takes the server to complete a task (server think time), place a NAM close to the server. Doing so will give you the most accurate reading on how long it took the server to respond. If you want to gather information about both server think time and the time it takes the network to transmit the data (flight time), then place another NAM close to a client that uses the application on the server.

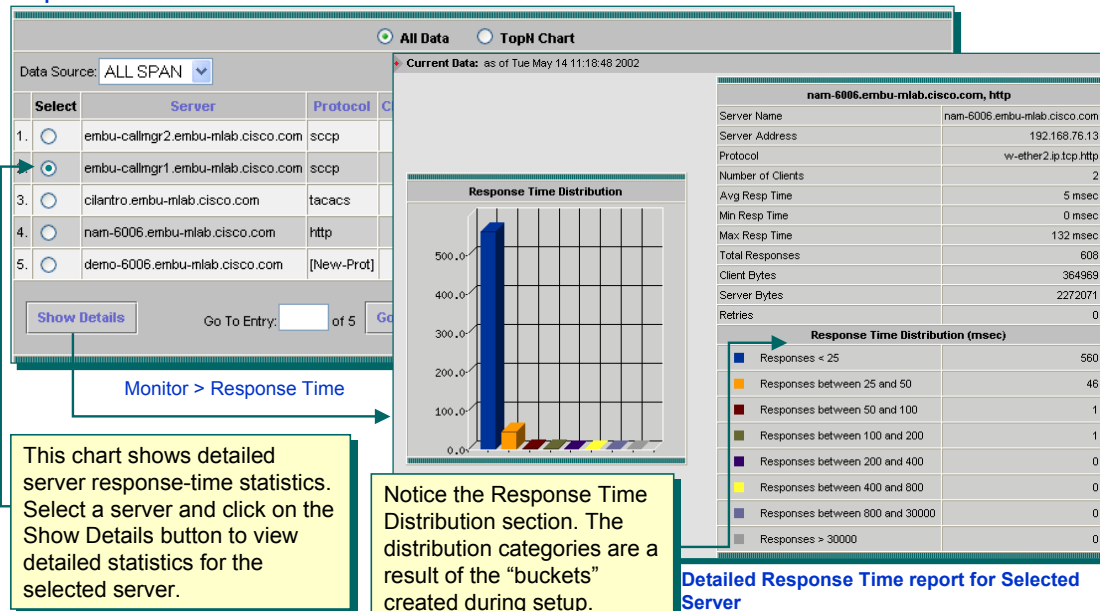
To configure this feature, choose Response Time Monitoring from the **Setup > Monitoring** menu. You will be given the option to choose which data source you want to monitor. Remember that on the NAM-1/2 if your SPAN session consists of ports or a Cisco EtherChannel® tunnel as your SPAN source, you must determine which VLANs your SPAN source belongs to. Editing the selected data source opens a dialog box which allows you to configure the resolution of the response-time samples and how the samples are reported. The report interval allows you to define the sampling interval, the amount of time to collect response-time samples. The next seven options are buckets that the NAM uses to store the results of the response-time samples for reporting purposes. For example, if a sample response-time measurement is determined to be less than 5 milliseconds (ms), then the NAM would increment the RSPTIME1 bucket by 1 and the NAM will report that sample as one response-time sample of less than 5 ms. As you can see, these options give you a lot of control over the granularity of response-time measurements and reporting you can configure. Let's look at a sample report of response time monitoring to clarify these points.

Note: Response time monitoring needs to see request-acknowledge pair to perform its analysis. Make sure the selected data sources are capable of seeing both packets.

Enabling Traffic Monitoring

Example: Response Time Statistics

Response Time All Data Table



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-99

Response Time Statistics

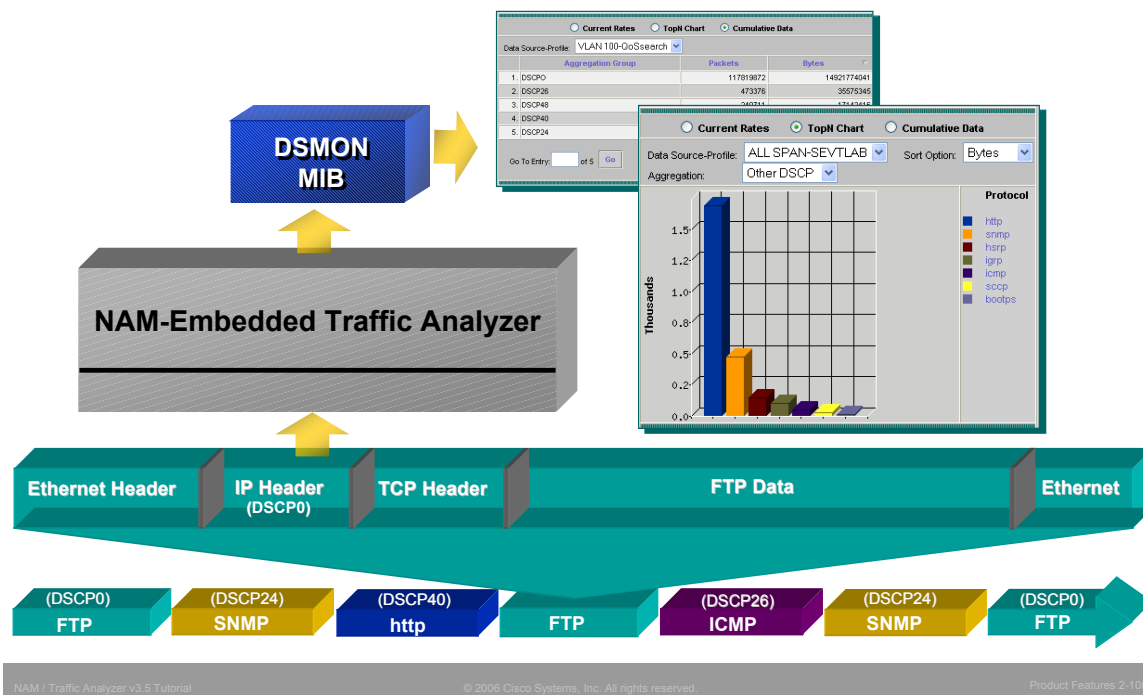
This illustration displays the monitoring reports that are generated when you enable Response Time Monitoring. The uppermost image shows you the first screen that appears when you go to the **Monitor > Response Times > Server** menu. This is a summary table that shows you statistics by server as seen by selected data source. If you select a server by clicking the radio button next to the server name and click the Show Details button, you will drill down into the detailed reports about the performance of your server based on response times. If you recall the discussion on time buckets, you will see that the NAM shows you how many samples fall into which time category. In the illustrated example, 560 individual occurrences of response times were less than 25 milliseconds. Let's say that we wanted to refine the collection because most of the samples occur below 25 milliseconds. We could then reassign the time buckets to smaller increments, say less than 10 milliseconds for the first bucket and 20 milliseconds for the second bucket, to get even more visibility into the performance of the server. As you can see, refining these buckets enables you to customize the data collection and reporting functions of the Traffic Analyzer software in the NAM to meet your reporting requirements.

Note(s):

- When you enable response-time monitoring, the NAM collects and reports the statistics for the interval you have defined, and the reports for the interval will not be displayed until the entire interval period has ended. So, if you have just enabled it, do not expect to see reports until after the entire interval period has passed.
- Changing the reporting interval can have performance considerations.

Enabling Traffic Monitoring

DiffServ Overview



DiffServ Monitoring Overview

The NAM also supports the ability to monitor and report DiffServ statistics using DSMON, a standard defined for monitoring Differentiated Services type traffic. Before we cover how to configure the NAM to monitor DiffServ, let's review a few basic DiffServ concepts.

DiffServ offers a method for implementing quality of service on a per-packet basis. In DiffServ, the 8-bit Type of Service (ToS) field in the IP header is replaced by the DS field, which identifies for DiffServ-enabled routers a value to determine how to handle the packet at each hop along a path. The first six bits of the DS field contain the DiffServ code point (DSCP). These 6 bits provide 64 different code points for defining how a forwarding device will handle the packet. In addition, classes are defined in DiffServ that determine how traffic in a class is handled and how resources within DiffServ-enabled routers are allocated on a per-class basis.

DSMON is MIB extension for monitoring DiffServ, and it offers statistics based on the code points defined in the DS field. The NAM offers the following DiffServ monitoring options:

- The percentage of traffic by DSCP—This can be used to validate your planning assumptions and implementation of quality-of-service (QoS) allocations.
- Protocols within a DiffServ DSCP—This can be used to detect incorrectly marked or unauthorized traffic.
- Protocol distribution within a DiffServ class—Again, you can use this to validate your QoS plan.
- Host statistics by DSCP
- Conversation statistics by DSCP and application.

Let's look now at the setup features for monitoring DiffServ.

Enabling Traffic Monitoring

DiffServ Overview – Aggregation Groups

User-Defined Profile



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-101

DiffServ Monitoring: Aggregation Groups

Enabling DiffServ monitoring is a simple process when you understand the steps and terms used in the configuration process. First, just two steps are involved in enabling DiffServ:

- Creating a user-defined profile
- Enabling DiffServ monitoring for a specific data source using a defined profile

A profile consists of one or more aggregation groups. An aggregation group is one or more DSCPs that use the same aggregation group name. It is simply a way of combining individual DSCPs into groups for consolidated reporting. What criteria you use to combine individual DSCPs into groups is up to you, because it affects how the NAM reports the data. To define aggregation groups and profiles, you must first identify what traffic has been assigned to the 64 DSCPs (0–63) you want to monitor for. When you know which DSCPs have been assigned, you can then put them into aggregation groups, if you choose. You can also use a non-aggregation scheme that essentially creates a single aggregation group for each DSCP. This setup allows the Traffic Analyzer to report on each DSCP individually.

Enabling Traffic Monitoring DiffServ Configuration

Setup > Monitor > DiffServ > Profile

DiffServ Monitor Profile		Last Modified
<input checked="" type="radio"/>	cisco-voice	Thu 21 Apr 2
<input type="radio"/>	QoSsearch	Wed 15 Jun 2005, 21:02:26 UTC

Existing profiles

Select a profile then take an action --> **Create** Edit Delete

Step 1: Define profile by assigning DSCPs to groups and giving the profile a name. Templates provide starting point.

Template: No Aggregation

Profile Name: QoSsearch

DSCP Value	Group Description
0	DSCP0
1	DSCP1
2	DSCP2
3	DSCP3
4	DSCP4
5	DSCP5
6	DSCP6
7	DSCP7
8	DSCP8
9	DSCP9

If DSCP is not named, then any traffic with this value will be reported as "other-DSCP"

Step 2: Enable monitoring functions to the profile you created in the previous step

Setup > Monitor > DiffServ > Monitoring

Data Source: Internal

DiffServ Profile: QoSsearch

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Traffic Statistics	Not applicable
<input checked="" type="checkbox"/> Application Statistics	100
<input checked="" type="checkbox"/> IP Host Statistics	100

Select an item then take an action --> Apply Reset

- You can assign a unique aggregation group description name for every DSCP value (as illustrated above) or you can assign the same group name to multiple DSCP values.
- DSCP values without an assigned aggregation group are placed into the "other DSCP" aggregation group.

Enabling DiffServ Monitoring

To create a profile, click on the **Create** button from the **Setup > Monitoring > DiffServ Profile** menu. This will bring you to the DiffServ Profile Setup screen. Enter a name for the profile. You can choose default templates that define aggregation groups for you or you can create a profile without using a template. After you have entered a group description for every DSCP value you want to monitor, click the **Apply** button at the bottom of the profile screen. Then, from the **Setup > Monitor > DiffServ Monitoring** menu, assign a DiffServ profile to a data source that you want to apply the DiffServ monitoring to. Finally, choose the monitoring functions you wish to apply to the profile and data source combination you just selected and click the **Apply** button. You must do this for every Data Source you wish to monitor DiffServ traffic for. Now let's look at some of the reports the Traffic Analyzer provides for DiffServ.

Enabling Traffic Monitoring

Example: DiffServ Statistics

You Are Here: [Monitor](#) > [DiffServ](#) > [Application Stats](#)

DiffServ Application Statistics

Per-Second Data: as of Tue 07 Jun 2005, 19:42:50 UTC

☒ Auto Refresh

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source-Profile: Protocol:

Aggregation: Showing 1-7 of 7 records

#	Protocol Name	Packets/s	Bytes/s	
<input type="radio"/> 1.	NAM-URL	13.05	9,107.38	92%
<input type="radio"/> 2.	snmp			
<input type="radio"/> 3.	netflow			
<input type="radio"/> 4.	icmp			
<input type="radio"/> 5.	http			
<input type="radio"/> 6.	not-name			
<input type="radio"/> 7.	snmptrap			

Rows per page:

Select an item then take an action --

Drill down on an application to see all conversations for that application with the selected DSCP value.

DiffServ application statistics provide application protocol statistics by data source and profile you created under [Setup > Monitoring > DiffServ Monitoring](#).

You Are Here: [Monitor](#) > [DiffServ](#) > [Traffic Stats](#)

DiffServ Traffic Statistics

Per-Second Data: as of Tue 07 Jun 2005, 19:44:35 UTC

☒ Auto Refresh

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source-Profile: Aggregation:

Showing 1-3 of 3 records

#	Aggregation Group	Packets/s	Bytes/s	
<input type="radio"/> 1.	DSCP0	4.80	2,325.90	99%
<input type="radio"/> 2.	DSCP48	0.10	9.40	<1%
<input type="radio"/> 3.	DSCP24	0.10	6.80	<1%

Rows per page: Units: Go to page: of 1

This table shows current data rates for aggregation groups (as defined in the QoS Search profile) seen on the data stream.

DiffServ Statistics

As illustrated, DiffServ monitoring provides reports on traffic, application, and host statistics by DSCP. You can use this information to validate your DiffServ configuration. You can also use this information, in combination with the response-time reports, to fine-tune your DiffServ implementation.

To further enhance your ability to monitor by DSCP values and ensure correct DSCP configurations, drill down on an application listed for a selected aggregation and DSCP to view associated conversation pairs. You can also drill down on a selected host from the [Monitor > DiffServ > Host Stats](#) menu to see all application conversations the selected host is having with DSCP values in the selected aggregation group.

Enabling Traffic Monitoring URL

Setup > Monitor > URL Collection

URL Collection configuration

Enable: ☒

Datasource: Internal

Max Entries: 100 Recycle Entries: ☒

Match only:

- ☒ Collect complete URL (Host, Path and Arguments)
- ☐ Collect Host only (ignore Path and Arguments)
- ☐ Collect Host and Path (ignore Arguments)
- ☐ Collect Path and Arguments (ignore Host)
- ☐ Collect Path only (ignore Host and Arguments)

Apply Reset

Enable URL collection, only one collection on a single data source can be enabled at a time.

- A URL, for example: <http://host.domain.com/intro?id=123> consists of a host part (host.domain.com), a path part (intro), and an arguments part (?id=123).
- The collection can be configured to collect all parts or it can be configured to collect only some of the parts and ignore others.

Monitor > Apps > URLs

Data Source: Internal URL Filter Clear

Showing 1-10 of 98 rows

#	URL	Hits
1	http://192.168.137.146/	1
2	http://192.168.137.146/admin/system/resources/overview.php	1
3	http://192.168.137.146/alerts/intro.php	1
4	http://192.168.137.146/auth/login.php	1
5	http://192.168.137.146/capture/intro.php	1
6	http://192.168.137.146/help/divva/%22+parent_relPath+%22shared/c	4
7	http://192.168.137.146/help/divva/%22+parent_relPath+%22shared/c	4
8	http://192.168.137.146/help/mappingfiles/divva_hlp.js	15
9	http://192.168.137.146/help/shared/content.css	2
10	http://192.168.137.146/images/abr_btn_hit_bg_08.gif	10

Rows per page: 10 Go to page: 1 of 10

Create URL-based Application

Set URL to be collected as an application/protocol

Enabling URL Monitoring

HTTP has become one of the most popular applications in use today. However, with many different web-based applications all using the HTTP port TCP-80, it makes it difficult to fully analyze and identify the traffic. To combat this, the NAM will collect hit statistics for every URL seen allowing you to analyze “web” traffic. To configure, select the **Setup > Monitor > URL Collection** task. In the displayed dialog box, select the data source to monitor URLs on (only one data source can be enabled at a time), select the maximum number of entries before overwriting the oldest, remembering that large tables use lots of memory, and select the portion of the URL to match on.

As will be seen later in this chapter, a URL can also be collected on as if it were an application. Thus instead of seeing HTTP traffic in application reports, you would see the URL as a separate application. A URL can be configured as an application from the URL monitor report **Monitor > Apps > URL** or from the **Setup > Protocol Directory** submenu as will be discussed next.

Enabling Traffic Monitoring Monitored Protocols

Setup > Protocol Directory > Individual Applications

Protocol Filter Clear

Showing 1-10 of 1668 records

#	Protocol	Identifier	Port Range	AddrMap Stats	Host Stats	Conv Stats	ART Stats
1.	AAA	40	1	n/a	✓	✓	n/a
2.	Competitive	16777221	1	n/a	✓	✓	✓
3.	Edonk	4662	1	n/a	✓		
4.	Soribada	22321	1	n/a	✓	✓	n/a
5.	SuperD	4661	1	n/a	✓	✓	✓
6.	WLSE	1741	1	n/a	✓	✓	✓
7.	[GUI]	5887	1	n/a	✓	✓	n/a
8.	[GUIprotocol]	1894	1	n/a	✓	✓	✓
9.	[HIB-IPX]	4	1	n/a	✓	✓	n/a
10.	Tues_Web	1045	1	n/a	✓	✓	✓

Rows per page: 10 Go to page: 1 of 167 Go

Select a protocol then take an action → Create Edit Delete

- The Protocol Directory shows you the protocols that are configured by default for collection and reporting.

(Support available in v3.5 for mobile wireless and SigTran protocols)

- Do not change these settings. If you have changes to make, add a new protocol, as shown.

Create New Protocol

Protocol Directory

Protocol Directory is a table that identifies what protocols the NAM recognizes and what statistics it gathers for each of those protocols. You can use this collection feature to add new protocols to the collection engine for analysis and reporting.

Most of the well-known protocols and ports are already defined for you, so you may find the best use of this feature is to add and monitor proprietary protocols that are specific to your environment.

Additional protocols have been added to the protocol directory to support mobile wireless, SigTran, and other well known protocols.

Enabling Traffic Monitoring

Monitored Protocols – Create New

New Protocol is encapsulated within :

- ☐ IP
- ☐ IPv6
- ☐ IPIP4
- ☐ GRE,IP
- ☒ TCP
- ☐ UDP
- ☐ Sun RPC (over TCP)
- ☐ Sun RPC (over UDP)
- ☐ IPX
- ☐ NCP

Step 1 of 2 -

< Back Next > Finish Cancel

Then choose from the list the protocol that the new protocol is encapsulated within. In our case, we chose TCP.

Then enter the TCP port that is assigned to the protocol. Also, define a name for this protocol and what statistics you want to gather.

New Protocol Parameters

L3 Encapsulation: IP

TCP port (0..65535): 51523

Name: w-ether2.ip.tcp.accountapp

Port Range (1-255): 5

Address Map ☐

Host ☒

Conversations ☒

ART ☒

Affected Stats:

Step 2 of 2 -

< Back Next > Finish Cancel

Application can be a contiguous block of ports

Protocol Directory – Create New

For example, let's say that you have a custom accounting application that uses TCP as a transport layer protocol, using TCP port number 50161. All you need to do is create a new protocol, identify its TCP port number, and define the statistics you want to collect. To do this, select **Setup > Protocol Directory** and click **Create** in the dialog box displaying the list of protocols the NAM is currently monitoring for. A dialog box will appear that allows you to choose the protocol that your proprietary protocol is encapsulated within. In our example, it is TCP. Click the radio button for **TCP** and click the **Next** button. This brings you to the second step of the create new protocol wizard that prompts you for, the TCP port number, the name you want to assign to this new protocol (that will appear in the Protocol Directory list illustrated above), and what statistics you want to gather for this new protocol. If this application actually used a range of continuous ports, you can also select the number of port to include after the entered TCP port. The end result is that the Traffic Analyzer will be able to differentiate this proprietary application by its TCP port(s) assignment and represent the application in the graphs and charts that provide application layer information.

Enabling Traffic Monitoring

Monitored Protocols – Auto Learned Applications

Setup > Protocol Directory > Auto-learned Applications

Autolearned Protocols Preferences	
Enable Autolearned Protocols:	<input checked="" type="checkbox"/>
Maximum Autolearned Protocols (100-500):	500
Maximum TCP Port (0-65535):	65535
Maximum UDP Port (0-65535):	65535
TCP Exclusion Port Range (0 Disables) (1-65535):	Start: 0 End: 0
UDP Exclusion Port Range (0 Disables) (1-65535):	Start: 0 End: 0
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The NAM will also detect new protocols and add them based on port number (i.e. TCP-1098 or IP-33).

Monitor > Apps > Individual Applications

☒ Current Rates
 ☐ TopN Chart
 ☐ Cumulative Data

Data Source: ALL SPAN
Filter
Clear

Showing 21-30 of 90 records

#	Protocol	Packets/s	Bytes/s	
<input type="radio"/> 21.	dns	0.04	4.82	<1%
<input type="radio"/> 22.	ntp	0.05	4.61	<1%
<input type="radio"/> 23.	mop	0.04	3.58	<1%
<input type="radio"/> 24.	disl	0.03	2.26	<1%
<input type="radio"/> 25.	tcp-4459	0.01	1.02	<1%
<input type="radio"/> 26.	tcp-4460	0.01	1.02	<1%
<input type="radio"/> 27.	tcp-4466			<1%
<input type="radio"/> 28.	tcp-4467	0.01	1.02	<1%
<input type="radio"/> 29.	tcp-4468	0.01	1.02	<1%
<input type="radio"/> 30.	tcp-4469	0.01	1.02	<1%

Auto-learned application

Rows per page: 10
 Units: Bytes/s
 Go to page: 3 of 9

Select an item then take an action -->
Details
Capture
Real-Time
Report

Auto-learned application

Protocol Directory – Auto-Learned Applications

The NAM can also be configured to “auto-learn” applications. For example, if the NAM saw packets using TCP port 2345 and had no corresponding protocol in the directory, it would then create and track a new entry TCP-2345.

Use the Setup > Protocol Directory > Auto-Learned Applications task to enable the auto-learning of application and limit them to maximum and by port range. After the maximum configured auto-learned applications are discovered, any new “unknown” protocols discovered will be aggregated together in an “others” bucket.

Enabling Traffic Monitoring

Monitored Protocols – URL Applications

Setup > Protocol Directory > URL-Based Applications

Index	Proto	Encap	Host Match	Path Match	Description
1	ipv4		192.168.1.159.196	/CCMApi/AXL/V1/soapisapi.dll	url-match-1
2	ipv4		http://192.168.159.118	/help/mappingfiles/divva_hlp.js	John
5	ipv4		192.168.1.159.118	/	Competitive
6	ipv4		192.168.1.159.196	/CCMApi/AXL/V1/soapisapi.dll	196_URL_Match
8	ipv4		www.cisco.com		tototo
10	ipv4		192.168.1.159.118	/admin/system/resources/overview.php	NAM-Resources
23	ipv4		192.168.1.159.118	/admin/users/accounts/accessLog.php	url-match-23
29	ipv4		http://www.sina.com	/	sina
34	ipv4			/soap/astsvc.dll	Andy-Test-34
50	ipv4		192.168.1.159.118	/images/otn_bg_1.gif	GIF

Select a protocol then take an action -->

Create Edit Delete

Collect and present statistics on a URL as an application.

Monitor > Apps > Individual Applications

Current Rates TopN Chart Cumulative Data

Data Source: ALL SPAN Filter Clear

Showing 1-10 of 34 records

#	Protocol	Packets/s	Bytes/s	
1	snmp	6.80	2,251.33	26%
2	hsrp	22.52	1,576.24	18%
3	tcp-unknown	6.00	1,260.00	15%
4	http	3.36	870.78	10%
5	Andy-Test-34	2.52	767.76	9%
6	ospf			9%
7	icmp			3%
8	arp	1.84	124.80	1%
9	sstp	1.48	106.73	1%
10	[nam-Prot]	0.15	82.04	1%

Rows per page: 10 Units: Bytes/s Go to page: 1 of 4 Go

Select an item then take an action -->

Details Capture Real-Time Report

URL-based application

Protocol Directory – URL Based Applications

URL-based applications are extensions to the protocol directory. So when the URL in an HTTP request matches the criteria of a URL-based application, the traffic is classified as that protocol.

A URL-based application can be used the same way as any other protocol in the protocol directory. For example, a URL-based application can be used in collections, captures, and reports.

So how does it work? An incoming URL is matched against the criteria of the configured URL-based application, in the order of the index, until a match is found. When a match is found, the remaining URL-based applications are no longer considered.

Previously, you saw how to create a “URL” protocol from the **Monitor > Apps > URLs** report. The **Setup > Protocol Directory > URL-Based Application** task will let you manually create, edit, and delete URL protocols. As illustrated above, selecting this task will present you with a list of already defined URL protocols. To define a new one, select the **Create** button.

Note(s):

- A URL consists of the following parts: a host, a path, and an argument. For example, in the URL `http://host.domain.com/intro?id=123`:
 - The *host* part is **host.domain.com**
 - The *path* part is **/intro**
 - The *argument* part is **?id=123**
- In the configuration of an URL-based application, the path part and the argument path are combined and called the *path part*. Enter the parts of the URL you wish to match to determine the URL protocol. An index must also be entered.

Enabling Traffic Monitoring

Monitored Protocols – Application Groups

Setup > Protocol Directory > Application Groups

Application Group:

Showing 1-9 of 9 groups

#	Application Group
1.	CiscoNM
2.	Database
3.	File-Transfer
4.	Multi-Media
5.	Multimedia
6.	Peer-to-Peer
7.	Web
8.	email
9.	test123

Rows per page: 50 1 of 1

Select an item then take an action -->

Group applications together for reporting purposes.

Application Group Name: Database

Encapsulation: IP

Application:

Selected Applications

- sql*net
- sqlserv (udp)
- sqlserv (tcp)
- ms-sql-mon (udp)
- ms-sql-mon (tcp)
- ms-sql-ser (udp)
- ms-sql-ser (tcp)
- oracle-server (udp)
- oracle-server (tcp)

Add protocols to an application group.

Monitor > Apps > Applications Groups

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source: ALL SPAN

Showing 1-2 of 2 groups

Application Group	Packets/s	Bytes/s	
+ Web	6.03	1,123.36	12%
+ Multi-Media	1.23	88.67	1%

Rows per page: 50 Units: Bytes/s 1 of 1

Select an item then take an action -->

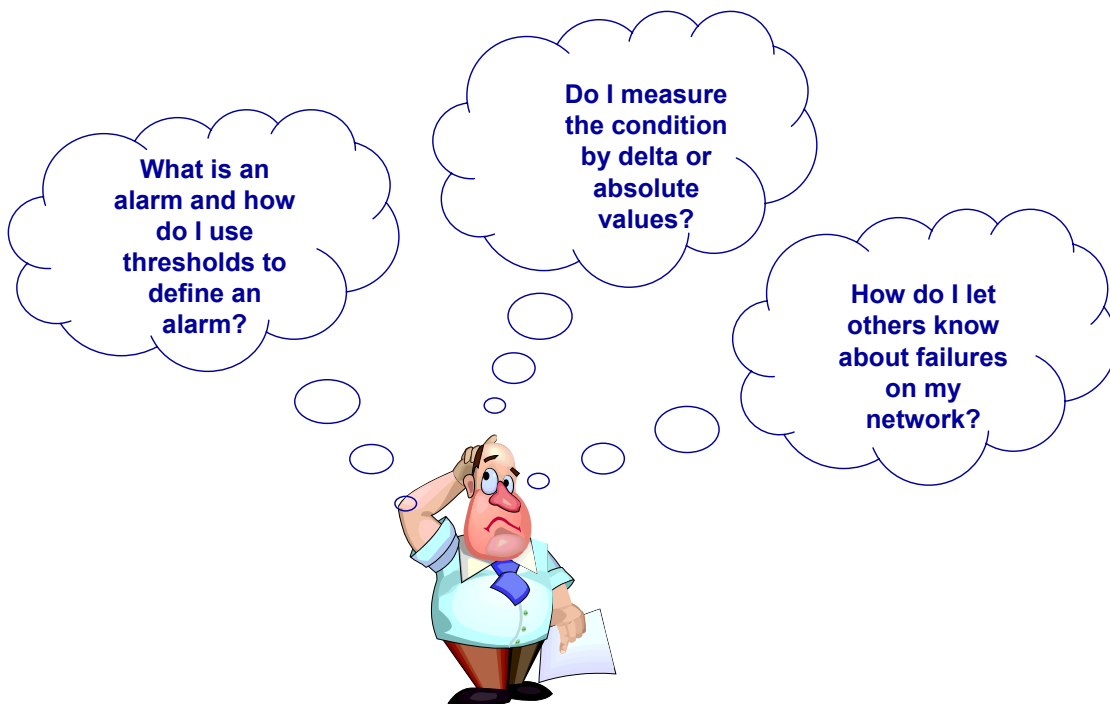
Protocol Directory – Application Groups

Applications (protocols) can be grouped together and viewed on reports as a whole. For instance, you could create a group called management that contains all management related protocols like SNMP, ICMP, etc. Now you can get an idea on how much bandwidth is being utilized for management as opposed to trying to determine this from each individual protocol.

To create an application group, select the *Setup > Protocol Directory > Application Group* task and click Create from the displayed list of currently defined application groups. Now simply give the group a name, and populate the group with the desired members for the list of available protocols displayed.

Use the *Monitor > Apps > Application Groups* report to view the application group usage.

Configuring Alarms Overview



Configuring Alarms Overview

Configuring alarms is serious business. This is because alarms are what network managers and engineers rely on to notify them when network or device performance falls below expectations. Alarms require a careful analysis of what variables are stored in the MIBs that will inform you of network and device problems and an equally careful implementation of those alarms. You may want to consider baselining your network to establish your expectations of normal behavior before you begin defining alarms. Another reason to carefully consider what alarms you need is because they consume NAM resources, and use of resources obviously can affect NAM performance. Before we get into the details of alarm configuration, let's review some terminology.








Alarm: An alarm is the condition that identifies when network or device performance falls below defined or normal expectations. You use thresholds (rising, falling, or both) to define the boundaries of your expectations. You set thresholds against MIB variables and with the NAM, you can set thresholds against RMON variables. There are different kinds of variables in MIBs, but the most common type you will encounter on the NAM is a counter variable. Counter variables work by incrementing the value in the MIB variable by one each time it sees a match for the variable. For example, if we use the variable Broadcast Packets, then every time the NAM receives a broadcast packet, it will increment the counter by 1. One way to use alarms with counter variables is to measure the difference (delta) between the value of the variable at the start and at the end of the sampling interval, thus reporting only the number of packets observed during the sampling interval. The other option for evaluating the data is by using the absolute value of the variable when it was read. For example, if the MIB variable for Broadcasts Packets had an absolute value of 33874 when sampled, then the NAM will report 33874 broadcast packets since the MIB variable was last cleared.

Event: An event is the actual occurrence of the condition you have defined in your alarm, such as when the network performance falls below your expectations. An event occurrence is stored in the MIB and is used for alarm reporting.

Trap: A trap is an SNMP message generated by the SNMP agent in the device that observed the event and is sent to the management station that has been configured to receive these traps.

Configuring Alarms

Types of Alarms

	NAM MIB Thresholds	Enables you to define thresholds/alarms based on byte or packet counts by protocol for network and MAC layer hosts and conversations
	NAM Voice Thresholds	Enables you to define thresholds/alarms for packet loss and jitter for SCCP, H.323, SIP, and MGCP
	NAM RTP Stream Thresholds	Enables you to define thresholds/alarms for packet loss packet loss statistics based on the RTP sequence number
	NAM Syslog	Enables you to store MIB and voice events as well as system alerts in either a local or remote syslog file
	Switch Thresholds	Enables you to define thresholds/alarms for variables stored in the mini-RMON agent of the switch; this includes variables such as port utilization, fragments, jabbers, alignment errors, collisions and more
	NAM Trap Destinations	Enables you to define the IP address and UDP port for the management station(s) that should receive notification of events generated by the Traffic Analyzer
	NAM Alarm Mail	Enables you to define email recipients that should receive notification of events generated by the Traffic Analyzer

NAM-1/2 Only

Types of Alarms

The Traffic Analyzer alarm features allow you to create alarms for a variety of the MIB variables stored in MIBs either on the NAM or on the switch. The following features allow you to create and customize alarms to meet your needs.

NAM MIB thresholds—NAM threshold MIBs enable you to create alarms and define thresholds based on byte or packet counter variables by protocol for network and MAC layer hosts and conversations. Additionally, MIB thresholds alarms can also be created for server response time, server client response time, DiffServ traffic statistics, DiffServ host statistics, and DiffServ application statistics.

NAM voice thresholds—NAM voice thresholds enable you to create alarms and define thresholds for packet loss statistics based on the RTP sequence number.

NAM RTP Stream thresholds—NAM RTP Stream thresholds enable you to create alarms and define thresholds for packet loss and jitter for SCCP, H.323, SIP, and MGCP.

NAM syslog configuration—syslog configuration enables you to send alerts as syslog messages to either a local or remote syslog file.

NAM switch thresholds—NAM switch thresholds enable you to create alarms and define thresholds for the variables stored in the mini-RMON agent of the switch. This includes variables for port utilization, fragments, jabbers, alignment errors, collisions, and more. This option is available on the NAM-1/2 only.

NAM trap destinations—NAM trap destinations enable you to define the IP address and UDP port for the management station(s) that should receive notification of events generated by the NAM.

NAM alarm e-mail—Allows you to forward alerts as e-mail messages to a list of defined recipients.

The next few pages cover these alarm options and how to create an alarm for event notification.

Configuring Alarms

NAM MIB Thresholds Alarm Configuration

Cisco Systems NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Switch Parameters Data Sources Monitor Protocol Directory Alarms Preferences

You Are Here: Setup > Alarms > NAM MIB Thresholds

NAM MIB Thresholds

Variable	Data Source	Address	Protocol	Code Point	Alarm Descr	Trigger Set
No alarm thresholds configured						

Select an item then take an action --> Details Create Edit Delete

Choose the analysis type

- In Packets
- Out Packets
- In Bytes
- Out Bytes

Choose what MIB variable you want to monitor on.

- Network Layer Host
- Network Layer Conversations
- MAC Layer Hosts
- MAC Layer Conversations
- Application Statistics
- Server Response Times
- Server-Client Response Times
- DiffServ Traffic Stats
- DiffServ Host Stats
- DiffServ Application Stats

MAC based alarms not available on NM-NAM

Choose the network protocol

- IP
- IPv6
- IPX
- Appletalk
- DecNet
- Vines

Next step is to choose alarm parameters

Next >

NAM MIB Threshold Alarms

Choose **Setup > Alarms** to enter setup mode for alarms. First, we will look at NAM MIB thresholds, so select that option from the menu in the upper left corner. Click the **Create** button and choose the variable from the pull-down list for the variable you want to alarm on. For NAM threshold alarms you will be given MAC or Network Layer Hosts, MAC or Network Layer Conversations, Application Statistics, Server or Client-Server Response Time, and Traffic or Host or application DiffServ Statistics as your variable options.

Next, choose the type of analysis you want to perform on the variable. The type of analysis depends on the MIB variable selected. For most NAM threshold alarms, you have the option of alarming by the number of received packets or bytes or transmitted packets or bytes. For Application based alarms the selection is either packets or bytes, and for the response time alarms the analysis selections include average, maximum, retries, timeouts, and bytes. You can also choose which network protocol you want to filter on (IP, IPV6, IPX, AppleTalk, DECNet, or Vines). Click **Next** to move to the next configuration screen to set the threshold parameters.

Configuring Alarms

NAM MIB Thresholds Alarm Configuration, continue ...

Select Parameters	
Data Source:	ALL SPAN
Network Protocol:	IP
Variable:	Network Layer Host InPkts
Network Address:	255.255.255.255
Polling Interval (seconds):	60
Description:	
Sample Type:	<input type="radio"/> Absolute <input type="radio"/> Delta
Rising Threshold (# of Pkts):	
Falling Threshold (# of Pkts):	0
Alarm Action:	<input type="radio"/> Log <input type="radio"/> Trap <input type="radio"/> Log and Trap
Community:	
Capture Trigger:	<input checked="" type="radio"/> None <input type="radio"/> Start <input type="radio"/> Stop

< Back Next > **Finish** Cancel

Choose the data source to monitor for this threshold condition.

Various alarm types will allow you to select the application to configure the alarm against.

Parameters depend on MIB variable selected

Define the length in seconds for the collection interval.

Enter a name that describes this alarm.

Define the rising and falling thresholds. Remember to set both since the occurrence of one is required to reset the other.

Choose what action to take for the alarm: log the event, send a trap, or both.

Set the community string for the system that will be receiving the trap. (This community string must match the trap community string set in NAM Traps.)

Choose to trigger a packet capture when the alarm is triggered.

NAM MIB Threshold Alarms (Continued)

This illustration shows you the remaining configuration choices you must make to complete the alarm setup. The first option is for the data source. Before you can define a NAM MIB threshold, you must enable data collection first. The NAM MIB threshold alarms enable you to create alarms for hosts and conversations. Therefore, you must enable host and conversation statistics for every data source you want to configure an alarm on.

Note: Again, on the NAM-1/2 make sure that VLAN data source matches your SPAN source, whether you spanned a port, a VLAN, or a Cisco EtherChannel® tunnel. Also, if you want to apply this to multiple VLANs in your SPAN session, you must create alarms for each VLAN or choose ALLSPAN to apply the alarm to all the VLANs in your SPAN source.

Next, enter the parameters specific to the threshold type selected. For example, if Network Layer Host was selected, enter the network address for the device you want to alarm on. Then, define the interval—the length of time in seconds of the collection period—and a descriptive name for the alarm. You must also choose the sample type—Absolute or Delta. When you are using counters, you should almost always use Delta because it is used to measure the amount that the counter has increased during a sampling interval. Always set the value for the rising and falling threshold. Setting both threshold values gives you the option to reset (rearm) the alarm. The reason for this is because alarms are like binary switches, they are either on or off. When you turn an alarm on, it stays on unless you set another threshold to change the alarm from on to off. Rising thresholds serve to reararm falling thresholds, and falling thresholds serve to reararm rising thresholds. After you have set your thresholds, you must choose which action the alarm should take: log the event to the syslog, send a trap message to the management station configured to receive them, or both. If you choose to send a trap, you must enter the community string of the management station that will receive the trap. The community string must match the trap community string set in the [Setup > Alarms > NAM Trap Destinations](#). The NAM also gives you the capability to control a data capture on the data source upon receipt of the alarm. Click [Finish](#) to enable the alarm.

As you will see later in the tutorial, you can view the alarms for the NAM from the Alarms tab. Now, let's move on to creating voice alarms.

Configuring Alarms

Voice Alarms

The screenshot shows the NAM Traffic Analyzer web interface. The top navigation bar includes 'Setup', 'Monitor', 'Reports', 'Capture', 'Alarms', and 'Admin'. The 'Alarms' tab is selected. The breadcrumb trail is 'You Are Here: Setup > Alarms > NAM Voice Thresholds'. The left sidebar contains a tree view with 'IIM Voice Thresholds' selected. The main content area is titled 'IIM Voice Thresholds' and contains a table with the following data:

IIM Voice Thresholds		
SCCP	<input checked="" type="checkbox"/> Jitter Threshold (ms):	10
	<input checked="" type="checkbox"/> Pkt Loss Threshold (%):	1
H.323	<input checked="" type="checkbox"/> Jitter Threshold (ms):	150
	<input checked="" type="checkbox"/> Pkt Loss Threshold (%):	5
MGCP	<input checked="" type="checkbox"/> Jitter Threshold (ms):	30
	<input checked="" type="checkbox"/> Pkt Loss Threshold (%):	5
SIP	<input type="checkbox"/> Jitter Threshold (ms):	30
	<input type="checkbox"/> Pkt Loss Threshold (%):	5

At the bottom of the table are 'Apply' and 'Reset' buttons.

Choose the jitter and packet-loss threshold for any or all (SCCP, H.323, MGCP, and SIP)

Enable voice monitoring first, using **Setup > Monitor > Voice Monitoring**, before you can receive voice alarms using these defined thresholds

Configuring Voice Threshold Alarms

Configuring voice alarms is a simple process with the NAM.

First, choose which voice protocol you want to alarm on. Select either: SCCP, H.323, SIP, or MGCP.

For each protocol selected, set your jitter and packet loss threshold. Remember that jitter is measured in milliseconds and packet-loss is measured as a percentage of all packets. When these defined thresholds are crossed, events will be generated by the NAM and reported in the Traffic Analyzer under the *Alarms* tab.

Remember that voice monitoring must be enabled via **Setup > Monitoring > Voice Monitoring** before you can generate voice alarms.

Configuring Alarms

RTP Stream Alarms

The screenshot shows the Cisco Systems NAM Traffic Analyzer web interface. The top navigation bar includes tabs for Setup, Monitor, Reports, Capture, Alarms, and Admin. Below this is a breadcrumb trail: You Are Here: Setup > Alarms > NAM RTP Stream Thresholds. The main content area is titled 'IAM RTP Stream Thresholds' and contains a table with two rows: 'Number of Consecutive Packets Loss (1-10):' with a value of 5, and 'Packet Loss Threshold (10⁻⁶)(1-100):' with a value of 1. There is a checkbox labeled 'Enable Alarm' which is checked. At the bottom right of the table are 'Apply' and 'Reset' buttons. A left sidebar contains a list of links: NAM MIB Thresholds, NAM Voice Thresholds, IAM RTP Stream Thresholds (highlighted), NAM Syslog, Switch Thresholds, NAM Trap Destinations, and NAM Alarm Mail. A line points from the 'Set consecutive packet-loss value and packet-loss threshold' callout to the threshold input fields.

Set consecutive packet-loss value and packet-loss threshold

Enable RTP Stream Monitoring first, using **Setup > Monitor > RTP Stream Monitoring**, before you can receive RTP stream alarms using these defined thresholds

Configuring RTP Stream Threshold Alarms

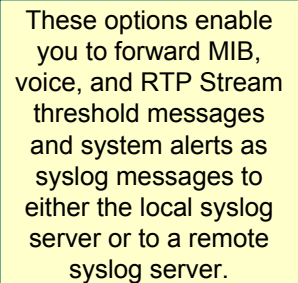
The NAM gathers packet loss statistics to monitor IP-based Video quality for applications such as Video on Demand and IPTV. Configuring RTP alarms is a simple matter of specifying how many consecutive packets lost will trigger an alarm, and configuring a packet loss threshold.

When the thresholds are crossed, events will be generated by the NAM and reported in the Traffic Analyzer under the *Alarms* tab.

Enable RTP stream monitoring first via **Setup > Monitoring > RTP Stream Monitoring** before generating RTP stream alarms.

Configuring Alarms

Syslog for the NAM



This option enables you to define up to five remote servers to forward alerts and messages to as syslog messages. You can use either IP address or host name in these fields.

Configuring Syslog for the NAM

The NAM syslog feature enables you to forward messages generated by the alarms to either the NAM syslog or to a remote server syslog file. This is a particularly useful feature because you can review these files to help identify patterns and repetition of problems and events on your network. CiscoWorks and other third-party systems support the parsing of syslog files for centralized event notification and monitoring. To enable this feature, choose the syslog file location, local or remote, for each of the three event types: MIB thresholds, voice, thresholds and system alerts. If you choose local, the NAM will store alert messages to its own syslog file. If you choose to log events and alerts to remote servers, enter either the IP address or IP host name for up to five remote servers. You can mix and match any combination of events with locations. For example, if you have a person dedicated to managing your voice system, you may choose to forward all voice threshold events to a server dedicated to voice management.

Configuring Alarms

Switch Thresholds Alarms

NAM-1/2
Only

Configuring a switch alarm is similar to configuring a NAM threshold alarm. The basic differences are the data source and the variable options.

Broadcast Pkts
Collisions
CRC Align Errors
Drop Events
Fragments
Jabbers
Multicast Pkts
Bytes
Oversize Pkts
Packets
Pkts size 64 Bytes
Pkts 65 to 127 Bytes
Pkts 128 to 255 Bytes
Pkts 256 to 511 Bytes
Pkts 512 to 1023 Bytes
Pkts 1024 to 1518 Bytes
Undersize Pkts

New Switch Threshold

Data Source: 2/1

Variable: CRC Align Errors

Interval (seconds): 60

Description: CRC Align Errors 2/1

Sample Type: ☐ Absolute ☒ Delta

Rising Threshold: 5

Falling Threshold: 0

Alarm Action: ☒ Log ☐ Trap ☐ Log and Trap

Community: public

Submit **Reset**

CISCO SYSTEMS

NAM Traffic Analyzer

Setup Monitor Reports Capture

Switch Parameters Data Sources Monitor Protocol Directory

You Are Here: Setup > Alarms > Switch Thresholds

Switch Threshold Alarms

Variable	Data Source	Interval	Sample Type	Rising Threshold	Falling Threshold	Alarm Descr	Alarm Action	Trap Community
<input type="radio"/> Pkts 64 Bytes	Gi1/1	60	Absolute	60	20	Small Packet Size	Log	public
<input type="radio"/> Packets	Gi1/1	60	Absolute	10000	5000	aaa	Trap	cisco

Select an item then take an action -->

Save **Create** **Edit** **Delete**

Configuring Switch Threshold Alarms

Configuring switch alarms on the NAM-1/2 allows you to set alarms for the variables stored in the mini-RMON agent in the Cisco Catalyst® Switch. Using this option, you can create port-level alarms for utilization, dropped events, bytes, packets, broadcasts, multicasts, cyclic-redundancy-check (CRC) alignment errors, undersized frames, oversized frames, fragments, jabbers, and collisions. To configure alarms for these variables, simply choose the port you want to alarm on, the variable, sampling interval, a descriptive name, sample type, threshold definitions and values, alarm event or action, and the community string for the management console that will receive traps, if you configured the alarm to trap on the event. Remember that you must create a new alarm for every port you want to alarm on.

As you will see later in the tutorial, you can view the alarms for the switch from the Alarms tab.

Refer to the discussion on defining NAM threshold alarms for more information on each of these parameters or refer to the chapter on Alarms in the User Guide.

Configuring Alarms

Trap Destinations

The screenshot shows the NAM Traffic Analyzer web interface. The top navigation bar includes links for Setup, Monitor, Reports, Capture, Alarms, and Admin. The breadcrumb trail indicates the current location: Setup > Alarms > NAM Trap Destinations. The main content area displays the 'NAM Trap Destinations' configuration page, which includes a table with columns for Community, Address, and UDP Port. A callout box points to the 'Create' button, stating: 'Enter multiple destinations to receive traps generated by NAM alarms.' Another callout box points to the 'Set Trap Destination' modal form, stating: 'To configure trap destinations, enter the community string for the management console that will receive the traps, its IP address, and the UDP port that listens to for arriving traps.' The modal form shows the following values: Community: public, Address: 10.3.3.3, and UDP Port: 162. The form also includes Submit and Reset buttons.

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-118

Configuring Trap Destinations

One more step is required to complete the configuration of alarms within the Traffic Analyzer—configuring it to forward traps to a network management console. Configuring traps is also a simple process. All you need to do is gather some information—the IP address, the UDP port number, and the community string—for the management console that you have designated to receive the traps. Notice that you can configure the Traffic Analyzer to send traps to multiple destinations, all with the same (or different) UDP port number and community string.

Note: The well-known SNMP trap UDP port number is port 162.

Configuring Alarms

Alarm Mail

Cisco Systems NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Switch Parameters Data Sources Monitor Protocol Directory Alarms Preferences

You Are Here: Setup > Alarms > NAM Alarm Mail

Email Alarm

Alarm Mail Configuration

Send Mail on Alarm: ☐

Mail Alarm to: [Email server](#)

[Apply](#) [Reset](#)

Instructions

To receive NAM alarm, identify the receiver's ID as complete email address, such as jdoe@cisco.com. One or more email addresses, separated by space, can be entered.

Enter multiple e-mail addresses to receive an e-mail notification for NAM alarms

Configuring Alarm E-mail

Alternative to notification via syslog or trap, the NAM can be configured to send an e-mail to a list of recipients when an alarm occurs. To configure, use the **Setup > Alarms > NAM Alarm Mail** task to enable the feature and enter a comma separated list of recipients.

Setting Software Preferences

The screenshot shows the 'Preferences' page of the NAM Traffic Analyzer. The page has a top navigation bar with tabs: Setup, Monitor, Reports, Capture, Alarms, and Admin. Below this is a breadcrumb trail: You Are Here: Setup > Preferences. The main content area is titled 'Preferences' and contains a table of settings. Callouts point to specific fields:

- Entries Per Screen (1-1000):** A text input field with the value '40'. Callout: 'Use this field to customize the default number of rows in a table.'
- Refresh Interval (15-3600 sec):** A text input field with the value '300'. Callout: 'Use this field to customize how often the NAM refreshes the data that you view.'
- Number Graph Bars (1-15):** A text input field with the value '15'. Callout: 'Use this field to customize the default number of bars in a bar graph.'
- Perform IP Host Name Resolution:** A checkbox that is checked. Callout: 'Use this field to enable IP host name resolution for use of host names in tables and graphs.'
- Data Displayed in:** Radio buttons for 'Bytes' (selected) and 'Bits'. Callout: 'Use these fields to format data and numbers' (pointing to both 'Bytes' and 'Bits').
- Format Large Numbers:** A checkbox that is checked.
- International Notation:** Radio buttons for '1,025.72' (selected), '1.025,72', and '1 025,72'.
- CSV Export Monitor Entries:** Radio buttons for 'All' (selected) and 'Current Screen Only'.
- Audit Trail:** A checkbox that is checked. Callout: 'Select this to enable Audit trail'.

At the bottom right of the form are 'Apply' and 'Reset' buttons.

Setting Preferences

Now that we have covered the configuration options available to you for data collection and reporting, let's look at some of the ways you can exercise some control over how the data is displayed. To do this, go to the *Setup > Preferences* menu. From this menu, you can customize how many rows of a table are displayed per screen from 1 to 1000. The default is 50. You can also configure the rate at which the Traffic Analyzer refreshes the data you view in Monitor, from 15 to 3600 seconds. The default is 60 seconds. You can also configure how many graph bars are displayed in TopN host graphs. You can also determine if you want the Traffic Analyzer to use IP host names rather than an IP address in the tables and graphs, then choose *IP Host Name Resolution*. Finally, you can set option to determine how numbers are displayed.

We have covered all the data collection options you have for configuring monitoring on your NAM. Now let's look at generating real-time and historical reports.

CISCO SYSTEMS



Network Monitoring Using NAMs

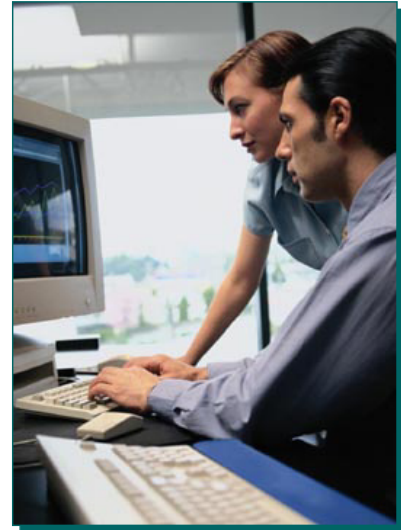
NAM Hardware Overview

➤ **Traffic Analyzer Software**

- Planning
- Getting Started
- Configuring
- Viewing Reports**
- Packet Capture and Decode



- **Viewing Real-Time Reports**
 - Types
 - Layout
 - Selecting Data Source
 - Common Error Messages
 - Standard Reports
 - Real-Time Trending
 - Drill-Down
 - Health
- **Creating and Viewing Historical Reports**
- **Viewing Alarm Logs**



Viewing Traffic Reports

In the previous section, we configured data collection for reporting as well as alarms and we also viewed some of the results of our configurations in the reports that the Traffic Analyzer generates. These reports can be found under the Monitor tab. If you wish to view the data long term, a historical report can be created causing the NAM to log the data to a database. The historical data can then be viewed from the Reports tab.

This section reviews in more detail the monitoring options found under the Monitor tab. In addition, it explores how the Traffic Analyzer lays out the reports for you in a drill-down sequence, how you can view the data by data source, the sub-tables on which monitor options are available to you, and what monitoring for voice and application response times are also available. This section also covers the ability to create and view historical reports and to view the alarm logs that store event messages generated from the alarms you configured in the last section.

Note: The use of reports is exactly the same for the NAM-1/2 and NM-NAM. The only differences is in the types of reports.

Viewing Traffic Reports

NAM-1, NAM-2 Report Types

Setup Monitor Reports Capture Alarms Admin	
Overview Apps Voice/Video Hosts Conversations VLAN DiffServ Response Time Switch MPLS	
Overview:	Combination of several statistics, including most active applications, most active hosts, protocol suites, and server response times
Apps:	Traffic statistics per application protocol (groups and URL)
Voice/Video:	VoIP (SCCP, H.323, MGCP, and SIP) and RTP stream monitoring
Hosts:	Traffic statistics per network host or MAC station
Conversations:	Traffic statistics per pair of network hosts or MAC stations
VLAN:	Traffic statistics per VLAN and VLAN priority
DiffServ:	Differentiated Service statistics
Response Time:	Client-Server application response times
Switch:	Mini-RMON and layer 2 statistics per enabled switch port and overall switch health
MPLS:	Traffic Statistics per MPLS tag

NAM / Traffic Analyzer v3.5 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-123

NAM-1, NAM-2 Report Types

From the Traffic Analyzer main menu, you can view all the reports that are available to you as a result of your data collection configuration choices made under the Setup tab. The reports for the NAM-1/2 include:

Overview—Offers an overview of performance that includes most active applications, hosts, protocol distribution, and response-time statistics. A good reporting option when you just want to see how things are running overall.

Apps—Gives you distribution statistics by application protocol. As discussed earlier, you can include your own proprietary protocols in these reports by creating a new protocol in *Setup > Protocol Directory*.

Voice—Reports under this heading include packet loss and jitter statistics for SCCP, H.323, SIP, and MGCP.

Hosts—Provides statistics by network and MAC layer host information. This option identifies which users are consuming valuable network and host resources.

Conversations—Provides statistics on network and MAC layer conversation pairs. You can use this option to identify which hosts are accessing which servers and use it when analyzing how increases in your user population may impact the load on server and network resources. You can also use these options to identify configuration errors on devices.

VLAN—Provides statistics by VLAN traffic and priority. From this menu, you can view resource utilization by VLAN priority (CoS) configuration.

DiffServ—Provides statistics by DSCPs for DiffServ-type traffic, hosts, and applications to verify DiffServ configurations.

Response Time—Provides detailed response-time graphs and tables by server and by client/server pairs.

Switch—Provides you with VLAN and layer 2 port level statistics, including utilization, errors, and broadcast statistics—always a good place to begin when searching for the cause of network problems.

MPLS—Provides you with basic in and out statistics for any MPLS flow defined as a data source.

Viewing Traffic Reports

NM-NAM Report Types

Setup	Monitor	Reports	Capture	Alarms	Admin		
Overview	Apps	Voice	Hosts	Conversations	DiffServ	Response Time	Router
Overview:		Combination of several statistics, including most active applications, most active hosts, protocol suites, and server response times					
Apps:		Traffic statistics per application protocol (groups and URL)					
Voice/Video:		VoIP (SCCP, H.323, MGCP, and SIP) and RTP stream monitoring					
Hosts:		Traffic statistics per network host or MAC station					
Conversations:		Traffic statistics per pair of network hosts or MAC stations					
DiffServ:		Differentiated Service statistics					
Response Time:		Client-Server application response times					
Router:		MIB-II and NBAR statistics per enabled interface and overall router health					

Viewing Traffic Reports NM-NAM

All Cisco NAMs offer the user a common experience. Thus, the NM-NAM report types are very similar to the reports of the NAM-1/NAM-2. There are some differences in the report types, however, due to the distinctions in the capabilities of both host platforms and NAM hardware platforms.

Viewing Traffic Reports

Monitor Report Layout

The screenshot shows the NAM Traffic Analyzer interface. Callouts highlight the following features:

- Select monitor report type.** Points to the 'Monitor' tab in the top navigation bar.
- Use the radio buttons to select report display view.** Points to the 'Current Rates', 'TopN Chart', and 'Cumulative Data' radio buttons.
- Print and data export options.** Points to the 'Print' and 'Export' icons in the top right corner.
- Some reports have context-sensitive submenus if they have more viewing options.** Points to the 'Network Hosts' submenu on the left-hand side.
- Choose your viewing data source here.** Points to the 'Data Source' dropdown menu.
- Most menus have a filter option to view a subset of data.** Points to the 'Filter' button next to the 'Data Source' dropdown.

The main display shows a table of network hosts with columns: #, Address, Via, In Packets/s, Out Packets/s, In Bytes/s, Out Bytes/s, and Non-Unicast/s. The table lists 10 hosts, including nmtg-hq-core-6506-nam.cisco.com and 192.168.137.85. The interface also includes a 'Per-Second Data' section, a 'Data Source' dropdown set to 'ALL SPAN', and a 'Filter' button. At the bottom, there are buttons for 'Details', 'Capture', 'Real-Time', and 'Report'.

Continued →

Monitor Report Layout

This figure offers a representative sample of the types of reports available to you. Once the main monitor report type is selected (Overview, Apps, Voice,...), you can select how the data is reported. Most monitor reports allow for the following display views: *Current Rates*, *TopN Chart*, and *Cumulative Data*. In this illustration, we are viewing the current rates for network hosts. We are shown the host and associated statistics for the host (Packets per second in/out, bytes per second in/out and non-unicast packets per second). If we selected the TopN Chart, we would see a bar graph representing the top hosts for one of the user selectable hosts statistics. Clicking on the column header of the Current Rates display will sort the table by that value. If we chose Cumulative Data, we would see a table similar to the one illustrated above, but with absolute total packets, bytes, and non-unicast packets received since the MIB counters were reset rather than the current rates.

Once selecting a report type, select the data source from the Data Source Pull down menu. Remember, earlier we talked about the pit falls of knowing what data sources are actually available and which have been enabled for data collection. You can further refine your view by selecting a network address to filter on.

Note(s):

- Only the data sources that were enabled for Network Host collection will appear in the pull down list.
- Some monitor reports have context-sensitive sub-menus (left-hand side of display) if there are more viewing options than those presented in the current view. In this case, you can obtain host statistics by either network or MAC layer addresses. We have shown you a view of network hosts only.
- All monitor screens provide the option to either print or export (in .csv format) the displayed data using the icons in the upper right-hand corner.

Viewing Traffic Reports

Monitor Report Layout (Continued)

Bottom portion of monitor report

The diagram shows the bottom portion of a monitor report interface. It includes a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 10, and a 'Go' button. Below this is a table with a header row containing a radio button and the text 'Select an item then take an action -->'. To the right of the table are four buttons: 'Details', 'Capture', 'Real-Time', and 'Report'. Callouts provide the following information:

- Rows to display per monitor report page:** Points to the 'Rows per page' dropdown.
- To use any of these options, first select a entry from the data table:** Points to the radio button in the table header.
- Details of selected item depend on monitor report. (i.e. details of host shows all applications and conversations by application for selected host) Details is same as clicking item in table row.** Points to the 'Details' button.
- Capture launches a data capture with a filter for the selected item from the monitor report data table.** Points to the 'Capture' button.
- Real-time launches a graph to track selected item over time.** Points to the 'Real-Time' button.
- Report creates a historical report and starts collection of data over time for the selected item from the monitor report data table.** Points to the 'Report' button.
- Use to display more pages of data.** Points to the 'Go' button.

Monitor Report Layout (Continued)

The bottom portion of many monitor reports provides additional display controls and options. Since screen space is limited, the user can control how many rows of data are displayed at once, and can easily jump to other pages.

As far as the display options, many will be discussed further later in the chapter but they are introduced here. To use any of these options, first select the desired row from the table displayed by clicking the radio button to the entries left. The additional display options are:

Details: Provides more information about the selected entry. This is a drill-down option and is the same as clicking the main object in the table entry (i.e. host from the hosts monitor report). The statistics displayed depend on the type of monitor report (i.e. details of host shows all applications and conversations by application for selected host).

Capture: Launches a data capture based on the selected table entry. (i.e. if a host is selected from the table with VLAN 100 selected, then a data capture is configured and started to look at the VLAN 100 data source and capture all packets to or from the selected host.)

Real-Time: Launches a graph that allows you to track the selected entry over time. (i.e. if a host is selected from the table, a graph will periodically update showing the current value of a host statistic selected by the user.)

Reports: Creates a historical report for the selected table entry and starts logging data about that selection to a database. The user can at a later time use the Reports tab to view activity for the selected item for up to 100 days from when the report was created. (**Note:** report will only have data as long as the selected item remains part of a configured data source.)

Next let's look at how to run monitor reports. Due to the large number of reports, not all reports will be discussed. Remember, many reports were already discussed in conjunction with the enabling of monitoring on the various data sources.

Viewing Traffic Reports

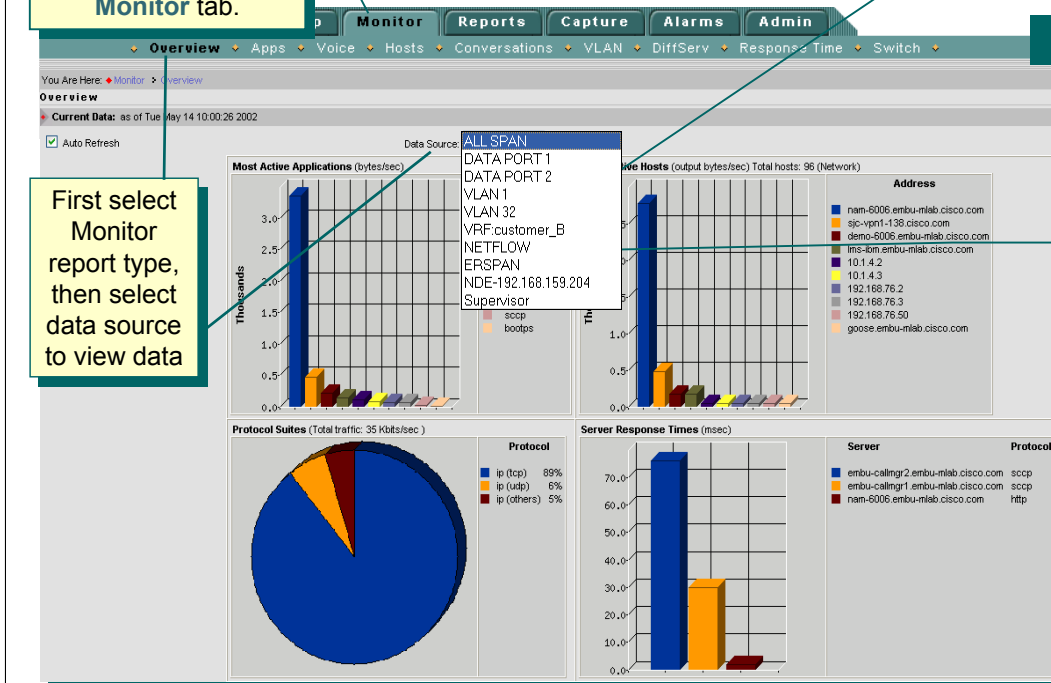
Selecting Data Sources

Real-time monitoring reports found under **Monitor** tab.

First select **Monitor** report type, then select data source to view data

The Data Source pull-down list shows you only the data sources that have been enabled for this collection using the **Setup > Monitor** task.

If the data source that you want to monitor is *not* on this list, begin by verifying that the VLAN/NDE is part of your configured data sources and that they have been configured for this type of collection using the **Setup > Monitor** task.



Selecting Data Sources

For most report generation dialogs, you will have at least two configuration options: your data source and whether or not you want to auto-refresh the report. The concept of data sources was discussed in detail in the Configuration section.

The important point to remember about viewing reports is that you will be only able to view Monitor reports for data sources that you configured to be sent to the NAM and have enabled for data collection. For example, the illustration shows ALLSPAN, DATAPORT1, DATAPORT2, VLAN1, VLAN32, VRF:customer_B, ERSPAN, NetFlow, NDE-192.168.159.204, and Supervisor as pull-down options on a NAM-1/2. These data sources are listed because they have been enabled for data collections from the **Setup > Monitor** task.

Note: The data sources listed here only mean that they have been enabled for data collection; it does not mean that they are currently one of the data sources being sent to the NAM for analysis. Therefore, remember to “clean up” the NAM configuration whenever the data sources are changed.

If you go to a report under the Monitor tab and the data source that you want to view reports on does not appear on the pull-down list, that is because you did not configure it for this type of data collection. To do so, you must go back to **Setup > Monitor** and configure the data source for this type of data collection. But before you do that, you must ensure that the data source you want to monitor is actually being sent to the NAM. If this is confusing, review the section on configuration again to complete these steps.

What do the data source pull-down options offer you? If you choose one of these data sources, the Traffic Analyzer will show you statistics for that data source only, enabling you to drill down to a report for a single data source.

You also have the option of enabling or disabling Auto Refresh. Auto Refresh tells the Traffic Analyzer to update the tables, graphs, and charts with new data as it receives it. Enable Auto Refresh when you want to see fresh data when it arrives, and disable it if you want to freeze a report view for any reason, perhaps while troubleshooting. The refresh rate can be set using the **Setup > Preferences** task.

Viewing Traffic Reports

Common Error Messages

The screenshot shows the Cisco NAM Traffic Analyzer web interface. The top navigation bar includes 'Setup', 'Monitor', 'Reports', 'Capture', 'Alarms', and 'Admin'. The left sidebar shows a breadcrumb trail: 'You Are Here: Monitor > Apps > Individual Applications'. The main content area is titled 'Applications' and shows 'Per-Second Data: as of Fri 08 Sep 2006, 10:40:12 PDT'. A 'Data Source' dropdown is set to 'VLAN 2'. Below this, a table header shows columns for '#', 'Protocol', 'Packets/s', and 'Bytes/s'. The table content displays 'No data available.' and lists 'Possible reasons: Data source not spanned to the NAM. Verify Setup > SPAN Sources; Initial data sample not yet complete. Refresh browser.; No recent activity on this data source.' At the bottom, there are controls for 'Rows per page' (40), 'Units' (Bytes/s), and a 'Go to page' field (0 of 0). A yellow callout box on the left contains the text: 'Another reason why you may have no data available is that, even though you configured the report, you chose a data source that is not part of the configured data source.'

Common Error Messages

There may be occasions when you choose one of the monitor reports and are presented with a screen that says that no data is available. Typically this indicates that collection was configured at one time, but the data source is no longer part of the input data stream to the NAM. It is important that the appropriate data collections are disabled when removing or changing a data source. There are occasions when the input data streams and data collections are configured correctly and still no data appears. This would usually indicate that no data of that type is present in the data stream.

Note: On the NM-NAM the External Data Source is configured for collection by default and will be displayed as a potential data source even if nothing has been connected to the port. If the external interface has not been connected, go to Setup > Monitor and disable all collections for the External data source.

Note: If this screen appears for response time reports and all configurations appear correct, check to make sure the input data stream contains both incoming and outgoing packets. Response time processing needs to see both the request (outgoing) and acknowledgement (incoming) packets to calculate the response time.

Viewing Traffic Reports

Standard Report Options

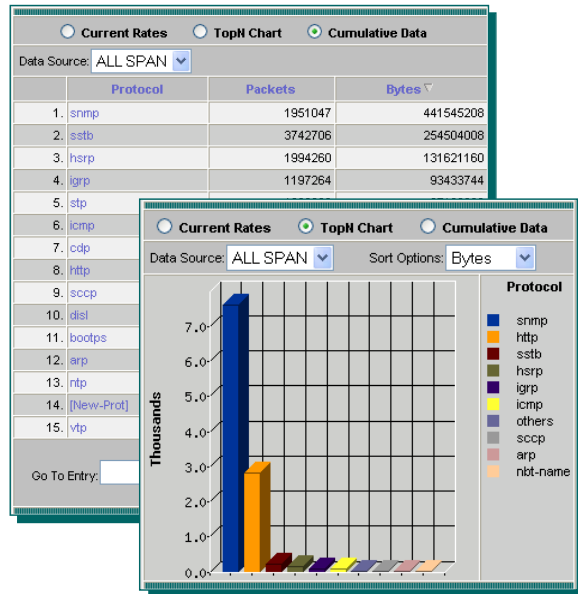
Current Rate Reports show data that has been collected during the most recent refresh interval only.

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data			
Data Source: ALL SPAN		Protocol:	<input type="text"/>
		<input type="button" value="Filter"/>	<input type="button" value="Clear"/>
	Protocol	Packets/s	Bytes/s
1.	http	5.21	3349.24
2.	snmp	4.28	1160.24
3.	sstb	3.10	211.03
4.	hsrp	2.24	147.93
5.	icmp	1.14	109.31
6.	igmp	1.34	104.90
7.	arp	0.66	41.93
8.	sccp	0.38	25.72
9.	bootps	0.03	11.93
10.	dns	0.07	10.28
11.	others	0.07	8.59
12.	nbt-name	0.03	3.31

Go To Entry: of 12

These three reports are available for application, hosts, conversations, VLANs, DiffServ, and port statistics.

Cumulative Data Reports show all data since the NAM started collecting.



TopN Charts shows the TopN entries for the selected statistic for the most recent refresh interval.

Standard Report Options

The Traffic Analyzer offers three reporting perspectives: Current rates, TopN charts, and cumulative data for almost every category of reporting: Application, hosts, conversations, VLANs, DiffServ, and port statistics. These reports offer the following details:

Current rates—This is the first screen that will appear by default when you choose a monitoring report from the Monitor menu. Current rates screen provides you with the values for *only* the most recent refresh interval. In other words, it gives you the difference (delta) between the value of the variable at the beginning and ending of the sampling interval. Current rate values are useful for identifying changes in usage from one sampling interval to the next, highlighting when a condition changes, either for the better or worse.

TopN Chart—This bar graph gives you a ranking of the top entries. Again, this chart gives you the top entries *only* for the most recent refresh interval. TopN charts are useful for identifying the network devices or applications that are currently consuming the most network resources.

Cumulative Data—Cumulative data gives you the absolute value of the variable you are looking at since the NAM started collecting statistics. This might be useful to you if, for example, you want to see how many broadcast packets have been observed since the NAM started collecting data. **Note:** the NAM-1/2 counters are cleared and reset to 0 when you execute the clear config command from the CLI of the switch.

Let's look at how to track a statistic in real-time.

Viewing Traffic Reports

Real Time Statistic Tracking

Monitor > Apps > Individual Apps

Current Rates TopN Chart Cumulative Data

Data Source: VLAN 99 Protocol: Filter Clear

Showing 1-10 of 12 records

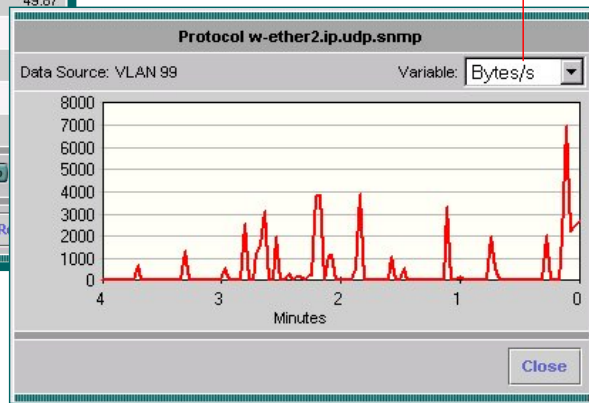
#	Protocol	Packets/s	Bytes/s
1. snmp		4.40	519.18
2. sstp		1.00	72.00
3. udp-16400		0.33	70.00
4. rtp		0.60	58.80
5. hsrp		0.72	50.17
6. icmp		0.53	49.87
7. telnet		0.63	
8. lgrp		0.43	
9. tacacs		0.18	
10. bootps		0.03	

Rows per page: 10 Go to page: 1 of 2

Select an item then take an action --> Details Capture Real-Time

How does the SNMP traffic on VLAN99 change over the short term?

Select statistic to track



Select table entry to track, and click the Real-Time report option.

Real-Time Statistic Tracking

The Current Rate report displays statistical values for the last refresh interval (set using *Setup > Preferences*) only. How can you view a statistic over time to monitor a trend? The Real-Time option button available at the bottom of many graphs will plot a selected statistic over the short period. As will be discussed later in this section, to track statistics over the long-term, use the Reports button to log the data to a database, and then view using the Reports tab.

For example, on a NAM-1/2 we wish to track the SNMP rate to the second floor devices. All SNMP traffic in this environment flows over VLAN 99. The SPAN is set up for port 2/1 – the uplink to the second floor. VLAN99 was then configured to enable application statistics collection. Viewing the *Monitor > Apps* report, the current SNMP rate can be viewed. Highlighting the SNMP entry in the table and selecting the *Real-Time* button launches a graph which begins to track SNMP over the short term.

Before looking at long term historical reports, let's first look at some of the drill-down reports available.

Viewing Traffic Reports

Application Drill-Down

Monitor > Apps > Individual Applications

Current Rates TopN Chart Cumulative Data

Data Source: ALL SPAN Protocol: Filter Clear

Showing 1-10 of 39 records

#	Protocol	Packets/s	Bytes/s
1. tcp-2428		48.00	3378.00
2. sstb		35.99	2587.55
3. tcp-3342		16.00	1188.00
4. hsrp		9.02	631.40
5. igmp		6.93	568.19
6. snmp		2.39	
7. icmp		0.81	
8. udp-16400		0.33	
9. stp		1.02	
10. ntp		0.64	

Rows per page: 10 Go

Select an item then take an action --> Details Captu

Drill down by application to see all hosts transmitting or receiving using that application.

Which hosts are generating specific application traffic

Hosts using w-ether2.ip.tcp.tcp-2428				
Host	In Pkts	Out Pkts	In Bytes	Out Bytes
10.1.6.101	149	147	10132	10878
10.1.6.103	234	232	16176	16742
10.1.6.109	149	147	10132	10878
192.168.76.233	233	286	16816	19712
192.168.76.243	295	348	21830	23664
192.168.79.42	100	0	6800	0

Close

Application Drill-Down

The Applications report gives you the ability to see which applications are consuming network bandwidth. Selecting any application (clicking the application or highlighting the entry in the table and clicking the *Details* button) allows you to easily determine which users (hosts) are responsible for consuming the bandwidth attributed to a particular application. This increases your visibility into consumers of network bandwidth to facilitate many network management tasks.

Note: Protocols discovered by the NAM but not listed in the Protocol Directory, are displayed and collected by port number as seen above – TCP-2428. See the information on Protocol Directory – Auto-Learned Applications presented earlier in this chapter for more information.

Viewing Traffic Reports

Application Group Drill-Down

Monitor > Apps > Application Groups

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data				
Data Source: DATA PORT 2 <input type="text"/> <input type="button" value="Filter"/> <input type="button" value="Clear"/>				
Showing 1-5 of 5 groups				
Application Group	Packets/s	Bytes/s		
<input type="radio"/> + Management	9.32	1,798.83	31%	
<input checked="" type="radio"/> + Router	15.16	1,176.14	20%	
<input type="radio"/> + Web	3.43	826.29	14%	
<input type="radio"/> + Multi-Media	0.60	43.20	1%	
<input type="radio"/> + Peer-to-Peer	0.00	0.17	<1%	
Rows per page: 50 Units: Bytes/s Go to page: 1 of 1 <input type="button" value="Go"/> <input type="button" value="Previous"/> <input type="button" value="Next"/>				
<input type="button" value="Details"/> <input type="button" value="Real-Time"/> <input type="button" value="Report"/>				

Drill down by application group to see all hosts transmitting or receiving using applications within the group.

Current Data: as of Wed 08 Jun 2005, 21:46:14 UTC					
Application Group Router					
Hosts using w-ether2.ip.udp.hsrp					
Description: Cisco Hot Standby Router Protocol (HSRP)					
Host	In Pkts	Out Pkts	In Bytes	Out Bytes	
nmtg-hq-dist-6509.cisco.com	0	822741	0	57591870	
nmtg-hq-dist-4006.cisco.com	0	411578	0	28810456	
192.168.159.177	0	2052735	0	143691450	
192.168.159.178	0	2052802	0	143696136	
192.168.159.193	0	3777585	0	264430950	
192.168.159.194	0	3777230	0	264406096	
ALL-ROUTERS.MCAST.NET	12894671	0	902626958	0	
Hosts using w-ether2.ip.ospf					
Description: Open Shortest Path First Interior GW Protocol (OSPF)					
Host	In Pkts	Out Pkts	In Bytes	Out Bytes	
192.168.159.69	0	11455	0	1193626	
192.168.159.98	0	76241	0	7081682	
nmtg-hq-dist-6509.cisco.com	23	280598	2298	26486868	
nmtg-hq-dist-4006.cisco.com	11	133254	1138	13932108	
192.168.159.177	46	698862	4596	65969496	
192.168.159.178	34	664226	3308	69405972	
192.168.159.193	42	1260791	4132	117875690	
192.168.159.194	30	1220665	2964	127338590	
OSPF-ALL.MCAST.NET	4450324	0	439619044	0	
<input type="button" value="Close"/>					

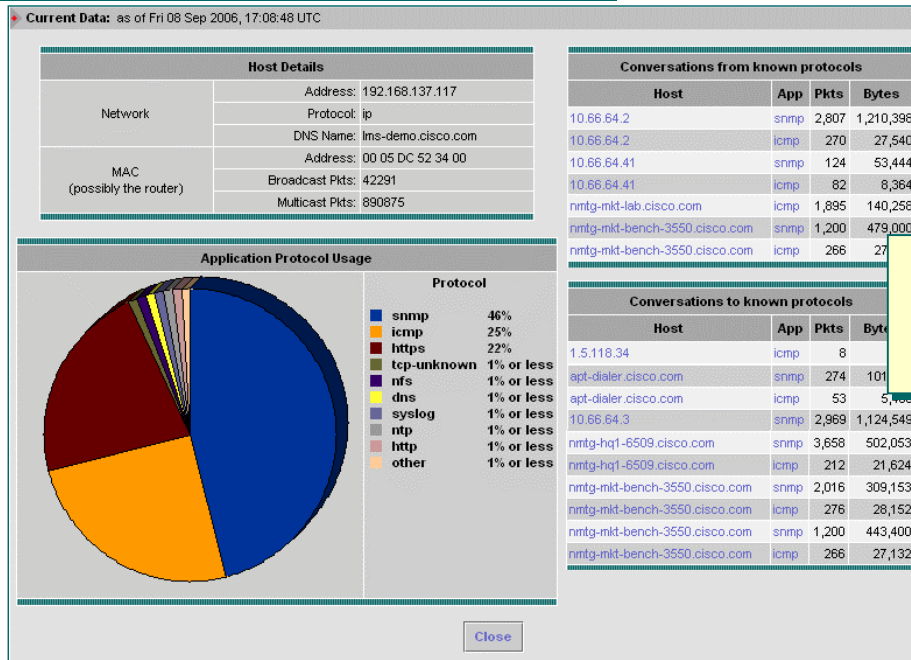
Application Group Drill-Down

The Applications Groups allow you to view bandwidth consumption of related protocols as opposed to looking for each protocol individually. Selecting any application group (clicking the application group and clicking the *Details* button) allows you to easily determine which users (hosts) are responsible for consuming the bandwidth attributed to each application that is part of the application group. This increases your visibility into consumers of network bandwidth to facilitate many network management tasks.

Viewing Traffic Reports

Host Drill-Down

From Host or Conversation report click on host or select row of table and click **Details** button



Details of network host activity and conversations by application

Host Drill-Down

A few of the Traffic Analyzer reports also enable you to drill down beyond the menu that you are currently viewing. Basically, any report table that has a host name in it provides the ability to drill down to more detailed information such as distribution of application protocols it uses, whom it shares a conversation with, and broadcast and multicast packets generated by the device. This report can be generated from either the Host or Conversation monitor report by either clicking on a host or selecting a row in the table and clicking the **Details** button. Experimenting with the report options will help you discover the ins and outs of the traffic reports.

Viewing Traffic Reports

DiffServ Drill-Down

Application Conversations - sccp Group - Voice Control			
Source	Destination	Packets	Bytes
10.1.1.100	192.168.76.233	7460	529648
10.1.1.100	192.168.76.243	1862	137788
192.168.76.199	192.168.76.196	140	9940
192.168.76.201	192.168.76.196	138	9798
Close			

Monitor > DiffServ > Application Stats

Drill down on an application listed for a specific aggregation group to see the conversations for that application

Monitor > DiffServ > Host Stats

Drill down on a host listed for a specific aggregation group to see the conversations and application protocol

Host Conversations - 192.168.76.233 Group - Other DSCP				
Source	Application	Destination	Packets	Bytes
10.1.6.101	mgcp	192.168.76.233	138	13524
10.1.6.101	tcp-2428	192.168.76.233	69	5106
10.1.6.103	mgcp	192.168.76.233	137	13426
10.1.6.103	tcp-2428	192.168.76.233	189	13390
Close				

DiffServ Drill-Down

Ensuring that the correct traffic and applications are transmitted with the desired DSCP value is paramount to correct QoS operation. A number of drill downs from the various DiffServ reports can help this cause. After correctly determining the proper protocols for a given aggregation group (one or more DSCP values) using the [Monitor > DiffServ > Application Stats](#) report, click on a application (or select the application and click the *Details* button) to see if any unexpected hosts are transmitting with this application and aggregation group.

You can also perform the reverse of the activity by first making sure the correct hosts are transmitting for a given aggregation group using the [Monitor > DiffServ > Host Stats](#) report, and then drilling down on a specific host to see if it is using the correct applications.

Viewing Traffic Reports

Voice Drill-Down

Monitor > Voice/Video > Voice Overview

Aggregate Statistics					
Protocol	Calls Monitored	Avg Pkt Loss (%)	Avg Jitter (ms)	Worst Pkt Loss (%)	Worst Jitter (ms)
<input checked="" type="radio"/> SSCP	3 K	0.00	0	0.00	0
<input type="radio"/> H.323	10	-	-	-	-
<input type="radio"/> MGCP	0	-	-	-	-
<input type="radio"/> SIP	0	-	-	-	-
Select a protocol then take an action -->					
Details					

Packet Loss and Jitter for the 5 "worst" calls.

- Voice Overview report provides an overview of packet loss and jitter statistics by protocol.
- Select **Details** to view packet loss and jitter by phone call.

Packet Loss - Worst Quality SSCP Calls								
Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter
<input type="radio"/> 33001	6022642001	John Johnson	-	Tue May 21, 2005 12:45:20 PM	10.1.2.100	10.1.6.101	0.6900	0
<input type="radio"/> 34002	33001	Les More	Susie Banshee	Mon May 20, 2005 04:39:25 PM	10.1.4.102	192.168.79.135	0.0100	0
<input type="radio"/> 41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/> 41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/> 33001	6022641001	John Johnson	-	Tue May 21, 2005 12:45:43 PM	10.1.2.100	10.1.6.101	0.0000	0
Select an item then take an action -->								
Details Clear								

Jitter - Worst Quality SSCP Calls								
Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter
<input type="radio"/> 41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/> 41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/> 33001	6022641001	John Johnson	-	Tue May 21, 2005 12:45:43 PM	10.1.2.100	10.1.6.101	0.0000	0
<input type="radio"/> 33001	6022642001	John Johnson	-	Tue May 21, 2005 12:45:20 PM	10.1.2.100	10.1.6.101	0.6900	0
<input type="radio"/> 33001	9192959001	John Johnson	-	Tue May 21, 2005 12:43:48 PM	10.1.2.100	10.1.6.101	0.0000	0
Select an item then take an action -->								
Details Clear								

To view individual call details

Continued

Voice Drill-Down

The Voice Overview report shows both packet loss and jitter for all calls since the NAM started collecting statistics. You can view the 5 "worst" calls as far as packet loss and jitter by selecting the protocol you want detailed reports on and then clicking on the **Details** button. You can also view voice statistics by all known phones as well as all active calls, which also provide packet loss and jitter statistics.

All Voice reports except for the Active Calls table reports display cumulative statistics for calls placed since the NAM was configured or the table was cleared. The Active Calls table shows only calls that are still in progress. Calls are aged out from the Active Calls table and other voice tables based on Least Frequently Used (LFU) configuration options you chose under the **Setup > Monitoring > Voice Monitoring** menu.

To see all details on a particular call, select the call from the appropriate report and click the **Details** button.

Viewing Traffic Reports

Voice Drill-Down (Continued)

Per call details

Current Data: as of Thu 28 Jul 2005, 22:39:42 UTC

SCCP call detail for calling party		
	Calling Party	Called Party
Number:	34002	32001
IP Address:	10.1.4.102	192.168.76.41
Call Reference:	17416680	
Owner:	Les More	Susie Banshee
Call State:	On Hook	
RTP Port:	22588	20128
Line Instance:	1	
Conference Id:	0	
Pass Thru Party Id:	4722929	
RTP Sampling Period:	20	
Payload Type:	G.711 ulaw 64k	

Page 1

Page 2

RTP Pre Value:	11
Silence Sup:	Off
Max Frames per Pkt:	0
G.723 Bit Rate:	-
Start Time:	Thu 28 Jul 2005, 22:36:43 UTC
End Time:	Thu 28 Jul 2005, 22:36:43 UTC
Packets Sent:	25580
Packets Received:	25577
Octets Sent:	4399760
Octets Received:	4399244
Packet Loss (%):	0.0100
Jitter (msec):	0
Switch Port:	-

Close

Voice Drill Down (Continued)

The illustration above is a drill down for a particular call displayed in the “worst” packet lost report. This report can also be displayed by selecting individual calls from the *Known Phones* drill down report or the *Active Calls* report.

Viewing Traffic Reports

RTP Stream Drill-Down

Monitor > Voice/Video > RTP Stream Traffic

Showing 1-2 of 2 records							
#	Source Address	Source Port	Destination Address	Destination Port	RTP Payload Type	SSRC Value	Packet Loss Rate 10 ⁻⁶
1.	172.20.104.34	23682	172.20.104.80	26010	PCMU	343262100	430
2.	172.20.104.80	26010	172.20.104.34	23682	PCMU	3421225620	0

Rows per page: 15 Go to page: 1 of 1

Select an item then take an action -->

Details

- RTP Stream Report report provides an overview of packet loss statistics to help assure a high rate of packet delivery.
- Select **Details** to view packet loss by stream.

Video Stream Details	
Source Address:	172.20.104.34
Source Port:	23682
Destination Address:	172.20.104.80
Destination Port:	26010
Payload Type:	PCMU
SSRC:	343262100
RTP Packet Count:	3137199
RTP Packet Loss:	1356
RTP Packet Loss Rate 10 ⁻⁶ :	432
Start Time:	Mon 28 Nov 2005, 17:33:42 PST
Last Timestamp:	859457856
Last Sequence:	10964
Close	

RTP Stream Drill-Down

The RTP Stream Traffic report shows the packet loss rate for configure RTP filters. You can view details of a stream by selecting the stream you want detailed reports on and then clicking on the **Details** button.

Viewing Traffic Reports

Server Response Time Drill-Down

Monitor > Response Time > Server

Server Response Time
 Latest Data: 180 second interval ending Thu 04 Aug 2005, 16:46:54 UTC
☒ Auto Refresh

☒ All Data ☐ TopN Chart

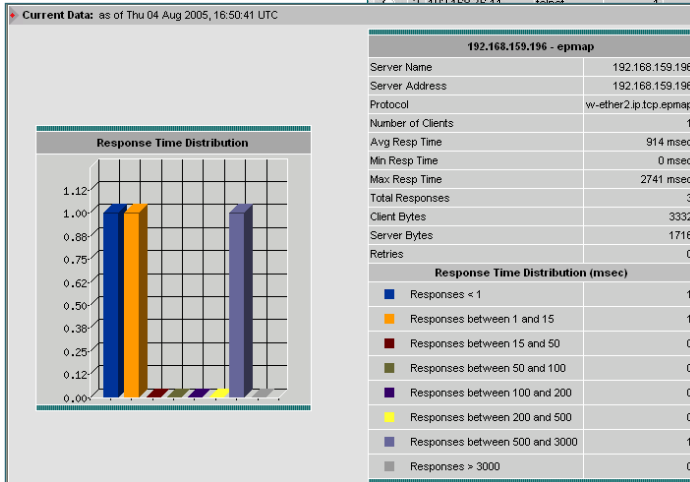
Data Source: ALL SPAN Server Filter Clear

Showing 1-5 of 11 records

#	Server	Protocol	Clients	Avg Resp Time	Min Resp Time	Max Resp Time	Retries	Late Responses
1	192.168.76.243	sctp	7	164	0	201	0	0
2	192.168.76.44	telnet	4	79	0	234	5	0
3	192.168.76.44	telnet	4	66	0	198	5	0
4	192.168.76.44	telnet	4	41	3	216	7	0
5	192.168.76.44	telnet	4	39	9	102	5	0

Go to page: 1 of 3

Details Capture Report



Detailed reports show the buckets you created during configuration to report on the individual response-time samples (for all client requests).

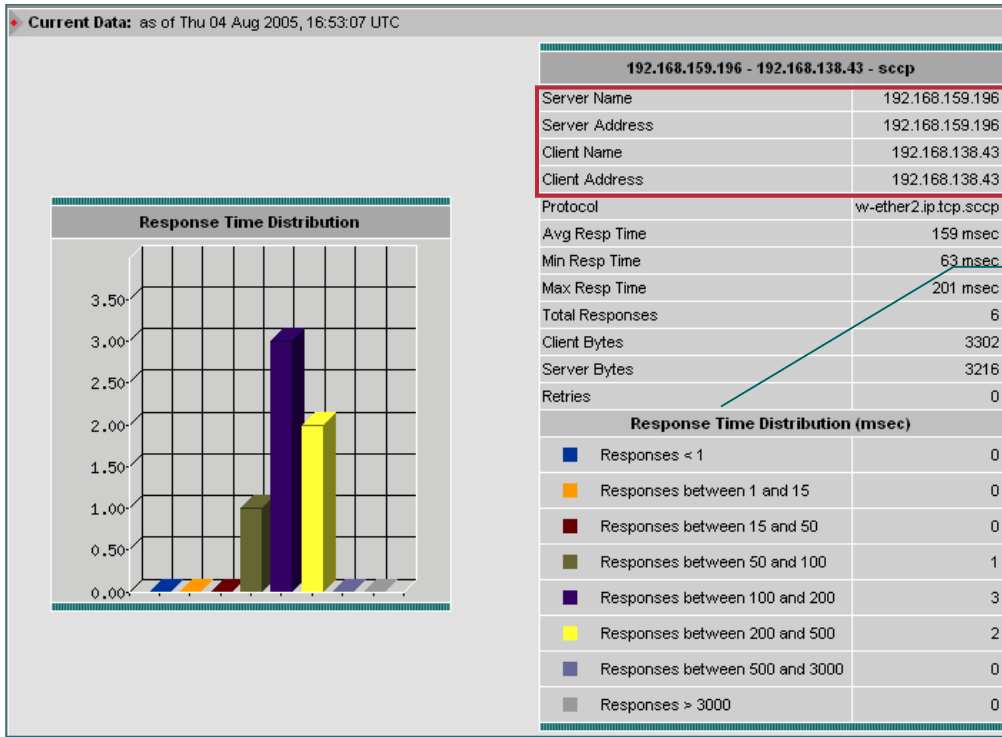
Server Response Time Drill-Down

As discussed earlier in the Response Time configuration section, depending on placement, the NAM reports statistics for either server “think” time (NAM placed close to the server) or request response-time (NAM placed close to the client - subtracting these two numbers would give you network “flight” time). The reports available for response time measurements fall into these two categories. If you want to view server-based statistics (the amount of time it takes a server to respond to all client requests), then view Server reporting. If you want to view statistics for individual client/server pairs, then choose Client/Server reporting. The Response Time reports for both client/server and server begin with an overview that provides minimum, maximum, and average response-times, as well as application protocol and the number of retries and late responses. As with most other views, you can use a filter to refine your views to an individual server. By default, the Traffic Analyzer shows you statistics for all server and client/server pairs, but you can also view response-times by TopN. Finally, you can select an individual server using the radio buttons to the left of the server name in either the Server or Client/Server menu and click the *Details* button to drill down to view more detailed statistics about the individual server or client/server pair.

If you select the radio button next to the server and click the *Details* button, you will be presented with more detailed information about the server performance for all client requests for a particular application. It includes the information provided in the Overview table as well as a distribution of the time samples into the buckets you defined during *Setup > Monitor*. It also gives you a bar graph of the distribution of time samples. This information is useful for gaining more visibility in the minimum, average, and maximum values and a clearer understanding of how well the server is performing.

Viewing Traffic Reports

Client/Server Response Time Drill-Down



Detailed reports show the buckets you created during configuration to highlight the individual client/server response-time samples.

Client/Server Response Time Drill-Down

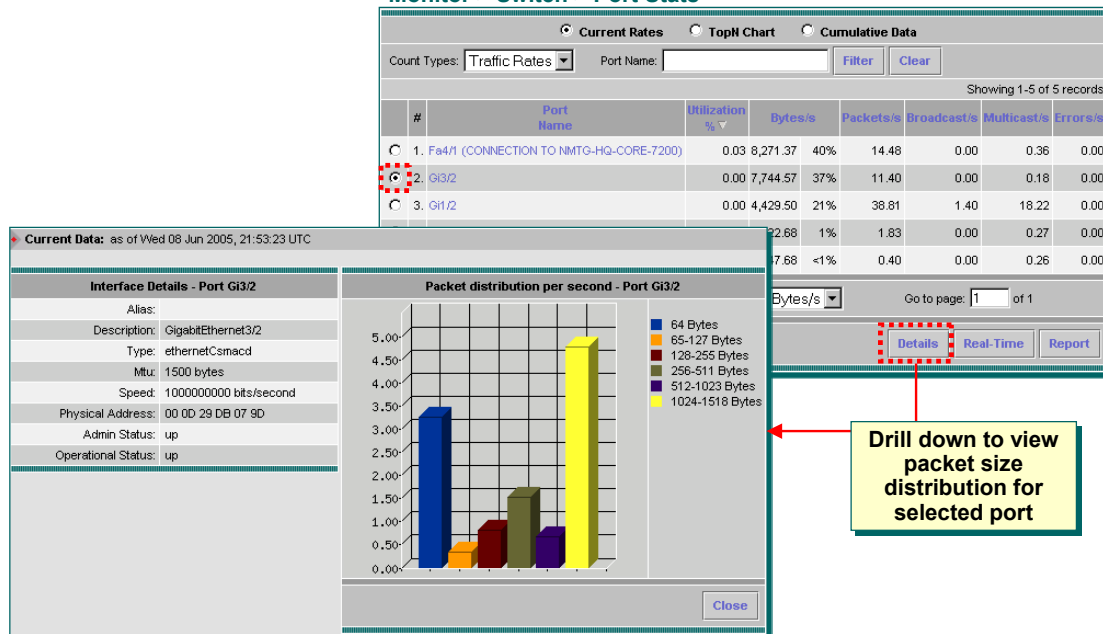
The format for reporting client/server response-times is virtually identical to the Server Response Time reports except it is reporting statistics based on a single client/server pair. The only real difference in the look of the two reports is that the Summary table includes a column for the client's IP host name or IP address. In all other respects, the format of these reports is the same. Remember, the Server report details the response-time statistics for all client requests to the server for a particular application, and the client/server report details the response-time statistics for a single client server pair for a particular application.

Viewing Traffic Reports

Port Drill-Down

NAM-1, NAM-2 Only

Monitor > Switch > Port Stats



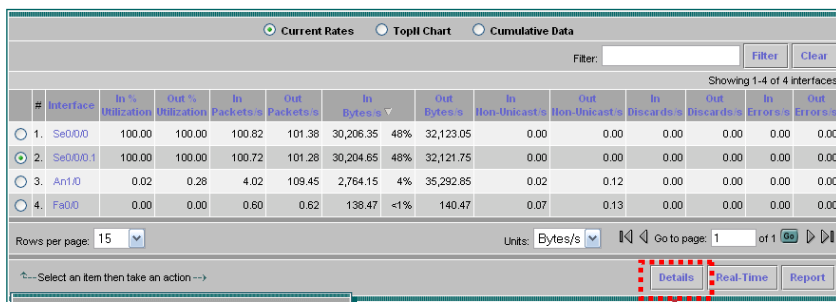
Port Drill-Down

On the NAM-1/2 the mini-RMON statistics pulled from the host switch provide utilization and error statistics for each active port. Selecting a port and clicking **Details** provides information about the selected port and also presents a packet size distribution.

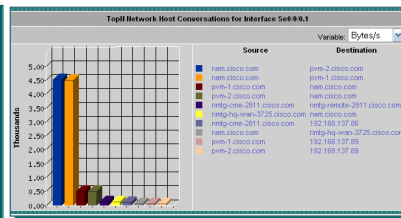
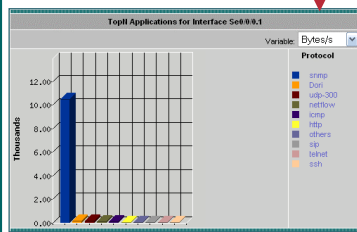
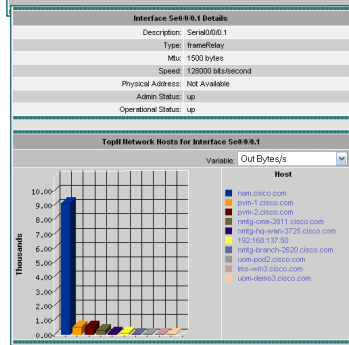
Viewing Traffic Reports Interface Drill-Down

NM-NAM Only

Monitor > Router > Interface Stats



Drill down to see
App, Host, and
Conv details for
selected interface



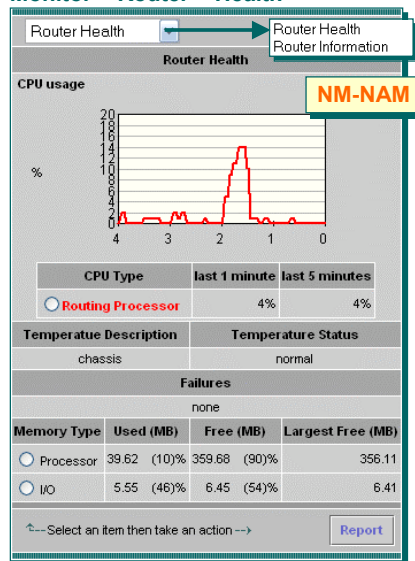
Interface Drill Down

On the NM-NAM interface statistics are pulled from MIB-II on the router. The administrator can also enable further RMON2 type analysis on each interface using the **Setup > Data Sources > Interfaces** configuration item. For enabled interfaces, the NAM configures NetFlow on the interface and sends the packets to itself. These packets can now be analyzed like any NDE data source. To see application, host, and conversation statistics for each enabled interface, select the desired interface and click **Details**. A table showing interface information and three graphs (one for each applications, hosts, and conversations) are displayed.

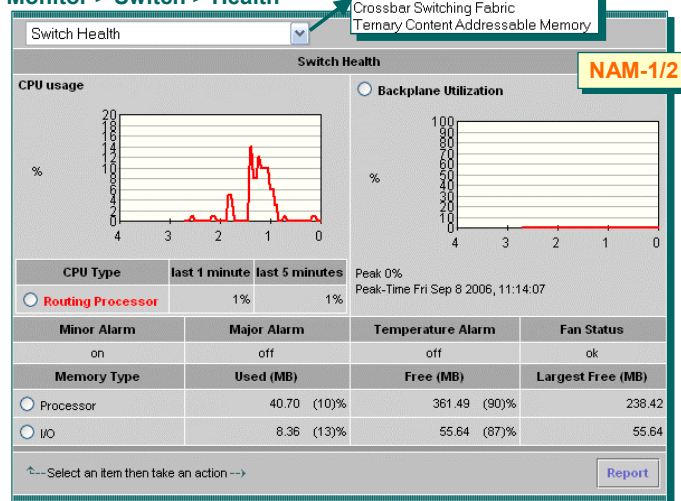
Viewing Traffic Reports

Router/Switch Health

Monitor > Router > Health



Monitor > Switch > Health



Router/Switch Health

As with all critical network devices, monitoring the overall health (CPU utilization, memory utilization, temperature, etc.) of a switch or router is important for keeping traffic flowing through the network and monitoring the impact to network devices when deploying new application services. When the Traffic Analyzer health report is run, the NAM will retrieve vital performance statistics from the host device and display them.

Besides Switch Health, the NAM-1/2 also includes health-based reports (pull down menu) covering Switch Information, Crossbar Switching Fabric, and Ternary Content Addressable Memory.

Besides Router Health, the NM-NAM also includes health-based reports (pull down menu) covering Router Information.

Next let's look at historical reporting.

Basic Historical Reports

Creating Report

The screenshot shows the NAM Reports interface. At the top, there are tabs for Setup, Monitor, Reports, Capture, Alarms, and Admin. Below these, there are sub-tabs for Basic Reports and Custom Reports. The main area displays a list of existing reports with columns for Name, Type, Data Source, Interval, Create Time, and Last Status. The 'Create' button is highlighted with a red dashed box. An inset window titled 'Select Report Type' shows a list of report types, with 'Applications' selected. The 'Next' button in the inset is also highlighted with a red dashed box. A red arrow points from the 'Create' button to the 'Next' button in the inset. A red arrow points from the 'Next' button to a red arrow labeled 'Continued'.

Existing Reports

Name	Type	Data Source	Interval	Create Time	Last Status
TCP	Appl Protocol - Bytes/sec	ALL SPAN	15 min	14 May 2005 13:20:27	OK
Top Ports - Utilization	Top Ports - Utilization %	-	15 min	14 May 2005 11:01:44	OK
Top Ports - Pkt Drops	Top Ports - Drop Events/sec	-	15 min	14 May 2005 11:01:45	OK

Historical Reports Controls

Select Report Type

Report Type: Applications

- Application Groups
- Hosts
- Conversations
- VLANs
- DiffServ
- Response Time
- Switch Ports
- Switch Health
- MPLS

Step 1 of 2 -

Back Next Cancel

Continued

Historical Reports

Earlier we looked at how to use the Real-Time graphs to do short term trending. Using the Historical reports we can extend this trending capability to up to 100 days from the creation of the report. It is important to remember that historical reports require a data source to be available for collection for the entire period of the historical report. If a historical report is created and the data source is completely changed, the data source for the historical report will no longer be available for collection. Similarly, if the collection options are changed, the NAM may no longer be collecting the necessary statistics for the report.

Historical reports are generated either from the Reports tab as illustrated above, or as shown in a few pages can be quickly created from one of the monitor reports. Let's first look at the creation of basic historical reports from the Reports tab.

Basic Historical Reports are created by selecting the **Create** button from the list of already created reports shown by selecting **Reports > Basic Reports**. Notice that the list of already created reports includes a column indicating the status of the report. Conditions other than "OK" may be due to the changing of the data source or types of collections enabled as already discussed.

Numerous types of basic reports can be created by selecting one of the following from the first step of the Basic Report generation dialog: Applications, Application Groups, Hosts, Conversations, VLANs, DiffServ, Response Time, Switch Ports, Switch Health, or MPLS Statistics and clicking **Next**.

Note: the NM-NAM reports will not include VLANs or MPLS, and will have Interface instead of Ports and Router Health instead of Switch health.

Basic Historical Reports

Creating Report, Continue ...

Select Report Parameters

Setup Report Parameters

☒ Application:

Encapsulation: IP

Protocol: snmp (udp)

☐ Top N Applications

Report Settings

Report Name: SNMP (UDP) ☐ Customized

Data Type: Bytes/sec

Polling Interval: 15 minutes

Data Source: VLAN 32

Step 2 of 2

< Back Next > Finish Cancel

Report by
Application or Top
N Applications

Available TopN Reports:

- Protocols
- Hosts
- Conversations
- MPLS Tags

Title auto-selected
or can be created
by user

Historical Reports (Cont)

The next step in creating the report is to select the type of report. There are two options –Top N and Basic.

The Top N report, in this case, will display the Top 10 applications for every time period, where as the Basic report will show the applications used over time.

Finish the report configuration by filling in the report parameters associated with the selected report type.

Tips:

- When selecting the data source, on the NAM-1/2, the list includes all VLANs known to the switch and not just the ones currently part of the data source.
- Remember to verify that the appropriate collection has been enabled for the selected data source and report type . For example, on the Application Protocol report, ensure that the selected data source is part of the data source being sent to the NAM, and that the Application Statistics collection option has been enabled.

Once the parameters have been selected and the **Finish** button clicked, the NAM will collect the appropriate statistic every Polling Interval and place the value in a database. After a hundred days of collection, the data will begin to be overwritten.

Basic Historical Report

Quick Create

Monitor > Apps > Individual Applications

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source: Protocol:

Showing 1-5 of 5 records

#	Protocol	Packets/s	Bytes/s
1.	netflow	0.15	114.43
2.	hsrp	0.72	50.17
3.	sstb	0.50	36.00
4.	igrp	0.43	35.53
5.	bootps	0.02	5.83

Rows per page: Go to page: of 1

Select table entry
and click report to
create a basic
historical report

Entry is Pending
until first data poll

Basic Report Type:

	Name	Type	Data Source	Interval	Create Time	Last Status
<input type="checkbox"/>	TCP	Appl Protocol - Bytes/sec	ALL SPAN	15 min	14 May 2003, 13:20:27	OK
<input type="checkbox"/>	NETFLOW (VLAN 99)	Appl Protocol - Bytes/sec	VLAN 99	15 min	23 Jun 2003, 15:39:18	Pending
<input type="checkbox"/>	HTTP	Appl Protocol - Bytes/sec	ALL SPAN	15 min	14 May 2003, 13:46:42	OK

Quick Create Basic Historical Report

The alternate way to create a basic historical report is to run a real-time monitor report, highlight a desired entry in the table displayed, and click the **Report** button.

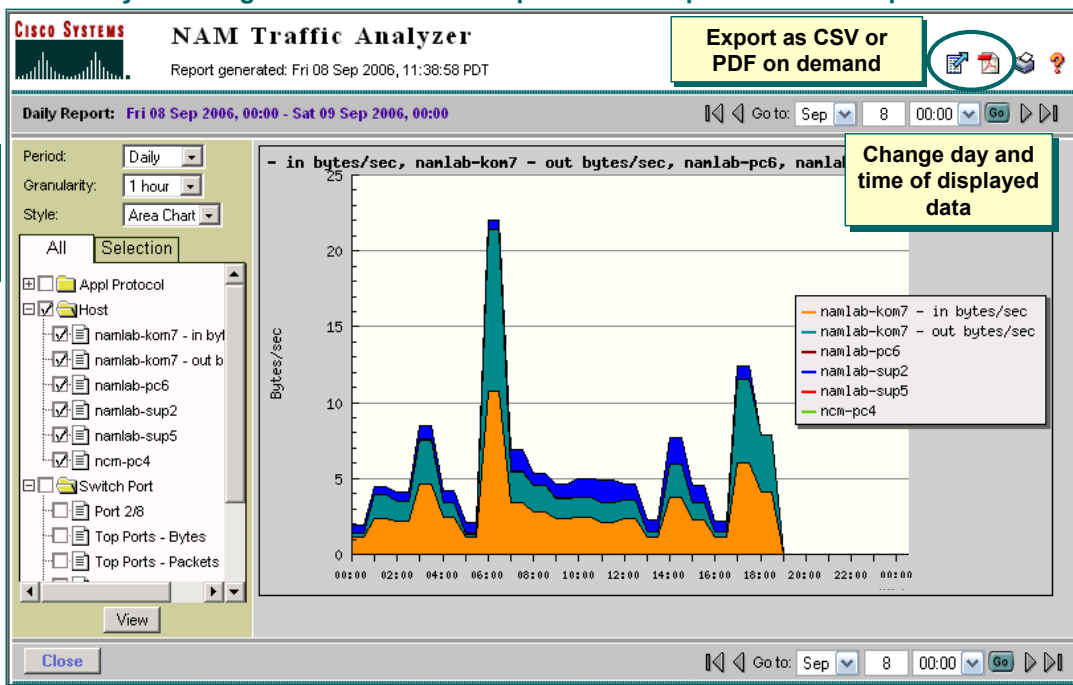
The benefit to creating a report in this manner is that you know that data is available for the desired data source and for the desired collection type. Remember that the default polling period of 15 minutes is used and a default statistic type is also used (bytes/sec, packets/sec, sec.) depending on the report type.

Now let's take a look at the reports generated and some of the display options.

Basic Historical Reports

Viewing Report

Launch by selecting one or more basic reports from Reports > Basic Reports



Change report period, granularity, and display style

List of all defined basic reports. Change report selection and click [View](#) to see another report

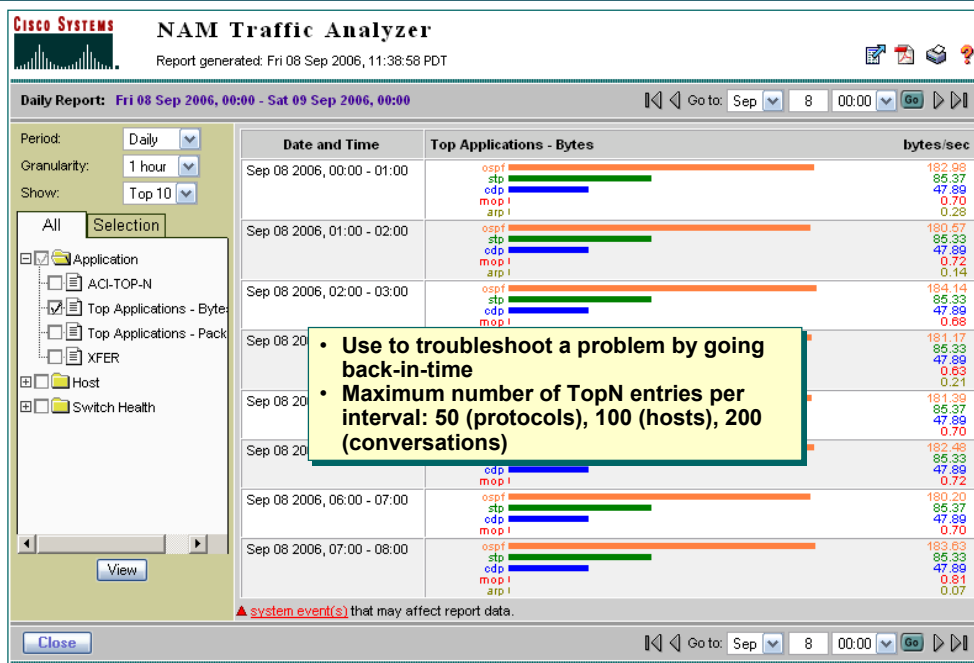
Viewing Basic Historical Reports

The Historical Reports are viewed in a separate window that once launched has an independent GUI from the main window of the NAM Traffic Analyzer. Launch the Historical Reports window by selecting one or more reports from the list displayed by selecting **Reports > Basic Reports** from the main NAM window, and clicking [View](#).

The left side of the report window displays a navigation tree of all created basic reports with the ones selected currently checked. Use this navigation to change which reports are being viewed. At the top left hand corner of the window, the user can select the period, granularity, and display style for the report. Of course the report can only display granularity no finer than the polling interval selected for the report during creation. By default, the period displayed is based on the current date and time, use the day and time option in either the upper or lower right-hand corners to change this.

Basic Historical Reports

Viewing Report – Top N



Viewing Top N Reports

The Top N Historical Reports are also viewed in a separate window that once launched has an independent GUI from the main window of the NAM Traffic Analyzer. The main difference in these reports is for each time period the Top N entities are displayed.

Basic Historical Reports

Create Custom Report

Reports > Custom Reports

Custom Reports	Last Modified	By User
<input type="checkbox"/> Default		

↑-- Select an item then take an action -->

[View](#) [Create](#) [Edit](#) [Delete](#) [New Folder](#)

Can create folders to organize custom reports

Used to group together basic reports

Report Name:

Folder:

Period: Granularity:

Style:

Report Data:

All Selection

- ☒ Appl Protocol
 - ☒ BOOTPS (VLAN 99)
 - ☐ HTTP
 - ☒ HTTP (VLAN 99)
 - ☒ NETFLOW (VLAN 99)
 - ☐ SNMP (UDP) (VLAN 100)
 - ☐ TCP
- ☐ Conversation
- ☐ Host
- ☐ Response Time

[Submit](#) [Reset](#)

Instructions

Use this form to combine and customize your basic report(s) to build a custom report.

You can combine multiple basic target reports but can select only one top-N report.

To move your custom report to a new folder, select a folder name in the list box before you click **Submit**.

Creating Custom Historical Reports

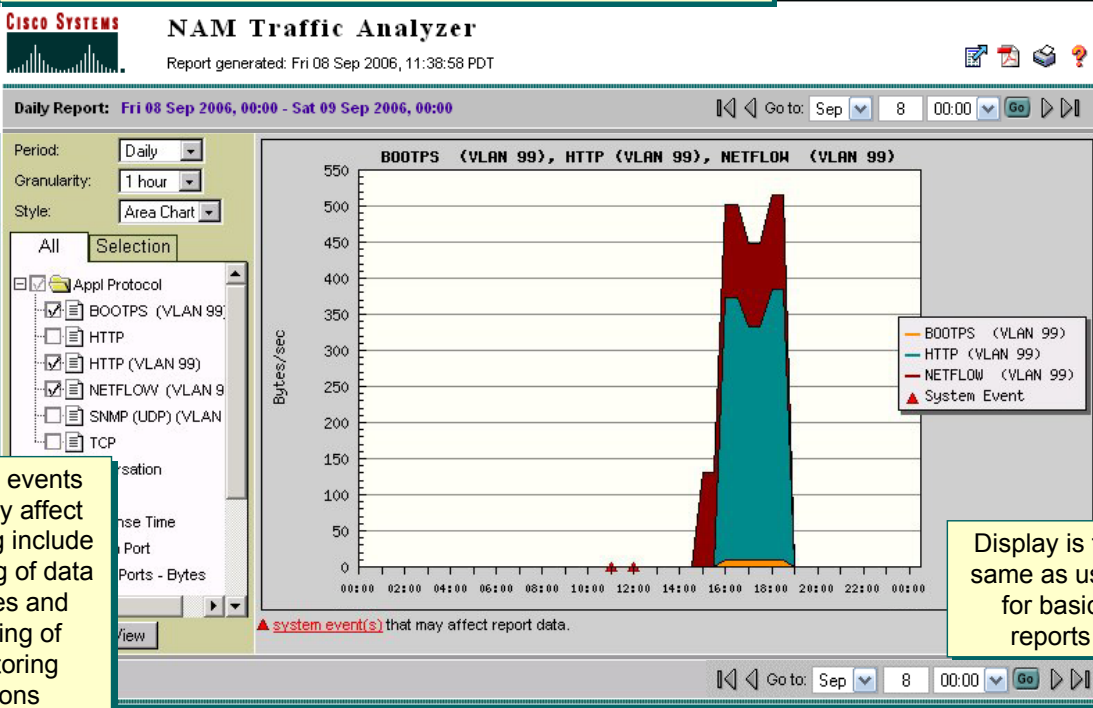
The second option available under the Reports tab is Custom reports. A Custom Historical report is simply a collection of basic reports displayed together. As seen previously, multiple basic reports can be selected for viewing; once the user finds a combination of basic reports useful for analysis purposes, they can then create a custom report to quickly launch this combination of basic reports.

To create a custom report, select **Create** from the dialog displayed by selecting **Reports > Custom Reports**. Notice that you can also create folders to help organize you custom reports. The Create Custom Reports dialog looks similar to the left-hand side of the Historical Report Viewing window. Simply select the basic reports to include in this custom report along with the period, granularity, and display style. Further give the report a name and put it into an already created folder for organizational purposes. Select **Submit** and the historical report will be created.

Basic Historical Reports

View Custom Report

Launch by selecting a report from **Reports > Custom Reports**



Viewing Custom Historical Reports

Custom reports are viewed in the same report window as the basic reports and are launched in a similar manner by selecting the custom report for viewing from the list displayed by selecting **Reports > Custom Reports** and clicking the **View** button. Since this is the same viewing window and GUI, all parameters of the report can be modified just like the basic reports (Custom reports is really just a short cut for selecting multiple basic reports).

One additional display item of importance to highlight is the system event indicator (small red triangle). This indicates that some system event has occurred (new SPAN source selected or collection options modified) that may impact the displayed data.

Basic Historical Reports

Scheduled Export

Reports > Scheduled Export > Create

The screenshot shows the 'Schedule Report - create' configuration window. It includes the following fields and callouts:

- Report Type:** Weekly Report (dropdown)
- Schedule Report On:** Day: Friday (dropdown), Hour: 17 (dropdown), Minute: 0 (dropdown). Callout: **Schedule report daily, weekly, or monthly**
- Report File Type:** PDF (selected), HTML, CSV, XML. Callout: **Select report format**
- Delivery Option:** Email (selected) with email address bob@company.com, or FTP Location (Select a Location dropdown). Callout: **Configure server using *Admin > System > E-mail Configuration* and FTP location using *Admin > System > FTP Configuration***
- Granularity:** 1 day (dropdown), **Style:** Top 10 (dropdown)
- Report:** A tree view showing folders like Application, Custom Reports, Host, and Switch Health. Under Application, there are sub-items like ACI-TOP-N, Top Applications - Bytes (highlighted), Top Applications - Packets, and XFER. Callout: **Select from existing reports**
- Buttons: Apply, Reset

Scheduled Export

The final option under reports is the Scheduled Export. Here one can configure the NAM to either e-mail or FTP (setup using the [Admin > System > Email or FTP Configuration](#) tasks) one or more existing basic or custom reports on a scheduled basis. Configuration is simple, select the reports to export, the format of the report, the delivery options, and the schedule.

Next let's look at the final report type to discuss, the alarm log.

Viewing Alarm Logs

NAM Thresholds

CISCO SYSTEMS NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

IIAM Switch

You Are Here: Alarms NAM

NAM Threshold Triggered Alarms

Current Alarms: as of Fri 08 Sep 2006, 14:31:26 PDT

☒ Auto Refresh

	Date	Time	Description	Variable	Alarm Value	Message
Showing 1-10 of 10 records						
1.	6 Sep	03:18:54	For Myself	protocolDistStatsPkts.30847.9766	0	FallingThreshold crossed
2.	6 Sep	03:17:54	For Myself	protocolDistStatsPkts.30847.9766	120	RisingThreshold crossed
3.	6 Sep	03:06:54	For Myself	protocolDistStatsPkts.30847.9766	0	FallingThreshold crossed

Rows per page: 40 Go to page: 1 of 1 Go

Clear

Viewing NAM Threshold Alarms

Under the Traffic Analyzer Alarm tab, you can view all the alarms that both the NAM and the Cisco Catalyst® Switch have generated. Remember, however, that alarms will appear only if you have first configured them under **Setup > Alarms**. Upon choosing the Alarm tab, you will be presented with two options:

- NAM, a link for displaying alarms generated by the NAM
- Switch, a link for displaying alarms generated by the Cisco Catalyst Switch (NAM-1/2)

This illustration shows the NAM's Alarm list with two alarms related to "Too many SNMP packets" as configured by the user. According to the description entered by the user, "too many SNMP packets" means greater than a 1000 in 30 seconds. As can be seen, the alarm was triggered because 1846 packets were seen in the 60 second interval. Notice that providing a good description can help you quickly determine the reason for the alarm. Use the **Clear** button to clear the table of alarms.

Viewing Alarm Logs

Switch Thresholds

NAM-1/2 Only

CISCO SYSTEMS

NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

NAM > Switch

You Are Here: > Alarms > Switch

Switch Threshold Triggered Alarms

Current Data: as of Fri 08 Sep 2006, 16:01:05 PDT

☒ Auto Refresh

	Date	Time	Description
1.	08 Sep 2006	14:39:37	"Greater than 60 pks/sec Gi1/3"
2.	07 Aug 2006	2:42:06	"Small Packet Size"

Display alarms detected on the Catalyst switch

A good description entered during setup can help pinpoint the exact nature of the alarm

Viewing Switch Alarms

If you choose the [Switch](#) link (NAM-1/2 only), you can view the alarms generated by the Cisco Catalyst® Switch. These alarms are a result of the switch threshold configuration choices you made under the [Setup > Alarms > Switch Threshold](#) menu. This log maintains up to 256 entries.

An event is fired when the alarm threshold set is met. The event stores the time of the event. If that same threshold is crossed again, a new event is generated and replaces the previous one in the log.

CISCO SYSTEMS

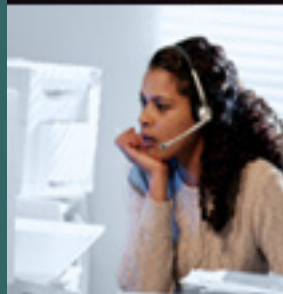


Network Monitoring Using NAMs

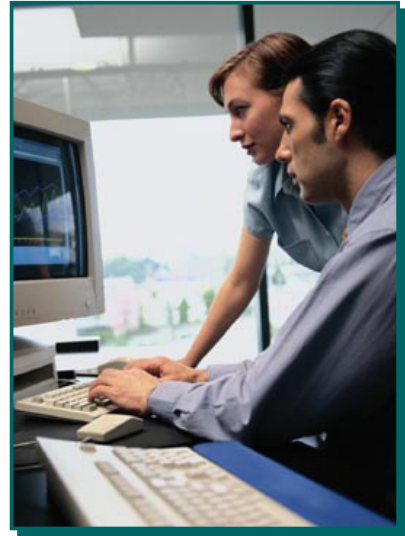
NAM Hardware Overview

➤ **Traffic Analyzer Software**

- Planning
- Getting Started
- Configuring
- Viewing Reports
- Packet Capture and Decode**



- Overview
- Buffers (NAM RAM)
- Capture Settings
- Quick Capture
- Decoding Captures
- Saving Buffers NAM Hard Disk
- Additional Remote Disk Storage
- Managing Capture Files



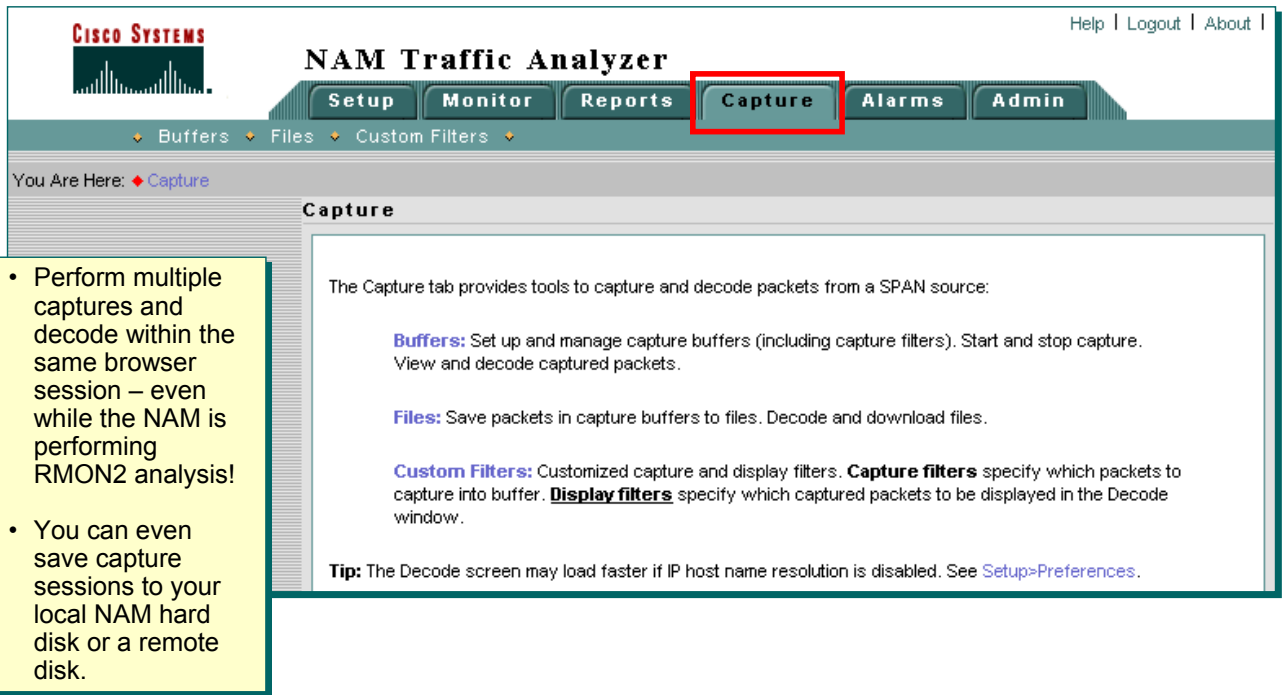
Packet Capture Overview

Previous sections discussed the NAM monitoring features that provide application visibility. As you may recall, the NAM does this by examining every packet that it receives, analyzing its layer 3, and upper-layer packet headers and storing the results of its analysis in the MIBs for reporting. With the NAM, you can also capture packets from any data source to view and analyze packets yourself. Packet capture, as this option is called, enables you to capture packets from a data source and view the details of the protocol information of each captured packet. To use this feature you must have already configured the data sources on the NAM. Then you define the data source to use and capture settings and filters. After you collect the data, you have the option to apply post capture decode filters to refine the presentation of the packets collected and to download the file.

This next section covers these features and how to use the Traffic Analyzer to perform your own packet analysis. Let's get started.

Packet Capture and Decode

Navigation Menu



The screenshot shows the NAM Traffic Analyzer web interface. The top navigation bar includes links for Help, Logout, and About. The main navigation menu has tabs for Setup, Monitor, Reports, Capture (highlighted with a red box), Alarms, and Admin. Below the navigation bar, there are sub-menus for Buffers, Files, and Custom Filters. The 'You Are Here' section indicates the current location is Capture. The main content area is titled 'Capture' and provides information about the Capture tab, including instructions on how to use Buffers, Files, and Custom Filters. A tip at the bottom suggests disabling IP host name resolution for faster loading.

- Perform multiple captures and decode within the same browser session – even while the NAM is performing RMON2 analysis!
- You can even save capture sessions to your local NAM hard disk or a remote disk.

The Capture tab provides tools to capture and decode packets from a SPAN source:

- Buffers:** Set up and manage capture buffers (including capture filters). Start and stop capture. View and decode captured packets.
- Files:** Save packets in capture buffers to files. Decode and download files.
- Custom Filters:** Customized capture and display filters. **Capture filters** specify which packets to capture into buffer. **Display filters** specify which captured packets to be displayed in the Decode window.

Tip: The Decode screen may load faster if IP host name resolution is disabled. See [Setup>Preferences](#).

Packet Capture - Navigation Menu

The packet capture feature enables you to collect packets from a data source that you have defined and then view the results of your collection, packet by packet.

The packet capture menu offers many options for filtering the packets you wish to capture and is easy to use. The options you need to consider when capturing packets are how much of the packet you want to capture (header and payload), as well as filtering options to limit the number of packets captured. You can filter traffic on a pre- and post-capture basis and, of course, you need to select your data source. When you finish capturing data, you can either decode it by viewing the capture or download the packets into a file for analysis by other third-party tools, such as application profiling and modeling tools. Alternatively, to expedite the capture configuration, many monitor reports allow you to select a table entry and use the contents as the basis for a capture configuration.

Packet Capture and Decode Buffers

Capture > Buffers

You Are Here: [Capture](#) > [Buffers](#)

Capture Sessions

Current Data: as of Mon 11 Sep 2006, 10:05:12 PDT

☒ Auto Refresh

Capture Sessions 300 MB total buffer memory 63.8 MB allocated 236.2 MB available

	Name	Owner	Start Time	Buffer Size	Packets	Status
<input checked="" type="radio"/>	HOST_192_168_159_7	LocalMgr	29 Aug 2006, 21:32:44	10 MB	43756	Locked
<input type="radio"/>	ART_192_168_137_86and10_70_230_81_http	LocalMgr	29 Aug 2006, 21:37:16	10 MB	0	Running
<input type="radio"/>	cvgCapture	LocalMgr	07 Sep 2006, 19:32:27	10 MB	50974	Locked
<input type="radio"/>	Capture1	LocalMgr	08 Sep 2006, 11:13:50	10 MB	463	Paused
<input type="radio"/>	COHVS_192_168_159_37and224_0_0_5	LocalMgr	07 Sep 2006, 19:38:34	10 MB	50973	Locked
<input type="radio"/>	Automatic_Capture	NAM Alarm (start capture)	29 Aug 2006, 02:23:58	10 MB	0	Running

↑ Select item(s) then take an action →

[New Capture](#) [Status](#) [Decode](#) [Save to File](#) [Delete](#) [Delete All](#)

Capture Buffers dialog shows all capture buffers (NAM RAM) and their current status

Create new capture

Modify selected capture buffer settings, pause, clear, and restart capture

Select buffer and decode packets

Save buffer to file on hard-disk, Use **Capture > Files** to view

Delete buffer(s)

Buffers

The NAM allows you to have multiple capture sessions running at once, therefore it is necessary to have a way of managing all the potential capture buffers. Executing the *Capture > Buffers* task presents you with a list of all currently defined buffers and their status:

Running--Packet capture is in progress.

Paused--Packet capture is paused. Captured packets remain in buffer, but no new packets are captured.

Cleared--Capture is stopped (by user) and capture buffer is cleared.

Locked--Capture is locked (stopped) because the buffer is full.

This information is important because Packet Capture utilizes memory and CPU and there is no sense leaving a buffer running or allocated if it is not necessary. From this screen the user can create new buffers (capture sessions), edit a buffer's settings including pausing and starting, Decode collected packets in a buffer, save the buffer to the NAM hard drive, and delete the buffer.

Let's take a look at these functions.

Packet Capture and Decode

Capture Settings

The screenshot shows the 'New Capture' dialog box in the NAM interface. The dialog is titled 'Capture Name: Capture2'. It has fields for 'Capture Status: Cleared', 'First Started:', 'Packets Captured: 0', and 'Buffer: Empty'. The 'Capture from:' dropdown is set to 'ALL SPAN', and 'Packet Slice Size (Bytes):' is 500. There are two main capture methods: 'Capture to Buffer' (with a 'Buffer Size (MB):' of 10 and a 'Wrap when Full' checkbox) and 'Capture to Disk' (with a 'File Size (MB):' of 100, 'No. Files: 1', and a 'Rotate Files' checkbox). The 'File Location:' dropdown is set to 'Local Disk'. The 'Capture Filter:' section has 'Include' selected. Below this are fields for 'IP Address' (Source, Source Mask, Destination, Dest Mask) and 'Both Directions'. There is also a 'TCP' section for 'Ports' and a 'Custom Filter' dropdown set to 'shay'. A 'Protocols' list on the right includes AAA, Competitive, Edonk, Soribada, SuperD, WLSE, and [GUI]. At the bottom are buttons for 'Start', 'Pause', 'Clear', 'Decode', and 'Close'. Callouts point to various elements: 'Status of capture' points to the 'New Capture' button; 'Select data source' points to the 'Capture from:' dropdown; 'Define how much NAM memory will be allocated to packet capture, or which disk (local or remote) to store data' points to the 'Capture to Buffer' and 'Capture to Disk' sections; 'Define how the NAM handles new packets when the buffer is full.' points to the 'Wrap when Full' checkbox; 'Capture filtering options enable you to filter out any unwanted traffic by address and/or protocol before it is stored in NAM memory for analysis.' points to the 'Capture Filter' section; 'Setup & use of remote storage discussed later' points to the 'File Location:' dropdown; and 'Capture controls, capture must be stopped to change settings.' points to the 'Start', 'Pause', 'Clear', 'Decode', and 'Close' buttons.

Callouts in the image:

- Status of capture
- Select data source
- Define how much NAM memory will be allocated to packet capture, or which disk (local or remote) to store data
- Define how the NAM handles new packets when the buffer is full.
- Capture filtering options enable you to filter out any unwanted traffic by address and/or protocol before it is stored in NAM memory for analysis.
- Setup & use of remote storage discussed later
- Capture controls, capture must be stopped to change settings.

Capture Settings

The first and most important configuration option for capturing data is your data source, which you do from the *Capture Packets from* field in the *Capture > Settings* dialog.

Capture to Buffer- As with all protocol analyzers, there is an absolute limit to the number of packets that the NAM can capture and store in memory, but it also has features to optimize the use of NAM resources while maximizing the number of packets stored. Those features include:

Wrap when Full —This option enables you to define what action the NAM should take when the buffer (RAM allocated for packet capture) is full: Should it *lock* the packet capture so that no packets get overwritten? Or should it overwrite (*wrap*) the oldest packets when the buffer becomes full?

Buffer Size—Here you have the option to define how much of the NAM memory you want to allocate to packet capture. Obviously, the more you choose here, the less you have for other NAM features and other Capture Buffers. Maximum buffer sizes: NAM-1 125MB, NAM-2 300MB, and NM-NAM 70MB.

Capture to Disk -Use to capture packets to disk instead of memory. You can select either the local NAM hard disk or any configured remote storage options. (Setup of the remote storage is discussed later in this section.) You can also select the file size, the number of files, and whether or not to rotate the files if all of them fill during capture or simply to end the capture.

Capture Filter—With this option, you can configure the NAM to ignore traffic before it is stored in memory. This is a very useful option if you have already narrowed the search for the source of the problem and you want to hone in on a specific subset of traffic. You can filter by protocol and/or by MAC or IP address for both source and destination addresses and add a mask to define which part of the address to include and which part to ignore. You can also define how you want the NAM to apply the filter—to include all packets that match the filter (inclusive) or exclude all packets that match the filter (exclusive).

Note(s):

- To change the capture settings you must first clear the capture buffer.
- You can use address and protocol filters together, but not port and custom filters.

Packet Capture and Decode

Quick Capture

Monitor > Conversations

Current Rates TopN Chart Cumulative Data

Data Source: VLAN 100 Source Filter Clear

Showing 1-10 of 194 records

#	Source	Via	Destination	Packets/s	Bytes/s	
1	nmtg-demo-2950.cisco.com	ip	nmtg-hq-access-3750.cisco.com	4.39	878.48	10%
		ip	item-ent-demo.cisco.com	1.11	496.07	5%
		ip	ALL-ROUTERS.MCAST.NET	6.83	478.34	5%
		ip	ALL-ROUTERS.MCAST.NET	6.83	478.34	5%

Units: Bytes/s Go to page: 1 of 20 Go

Details Capture Real-Time Report

Auto-name

Capture Name: CONVS_192_168_140_6

Capture Status: Cleared First Started: Buffer: Empty

Packets Captured: 0

Capture from: VLAN 100 Packet Size (Bytes): 500

Capture to Buffer: Buffer Size (MB): 10 Wrap when Full

Capture to Disk: File Size (MB): No. Files: 0 Rotate Files

File Location: Local Disk

Capture Filter: Include Exclude

☒ IP Address: 192.168.140.6 Source Mask: Destination: 192.168.159.169 Dest Mask: ☒ Both Directions

☐ TCP Ports: Port numbers: 0

☐ Custom Filter: shay MyFilter me

Start Pause Clear Decode Close

- From a monitor report, selecting a table entry and the **Capture** button automatically sets up a data capture using the table entry to fill in the capture settings.
- Note: Capture is immediately started and decode results are displayed.

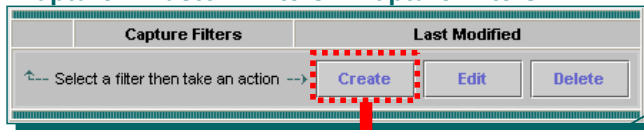
Quick Capture

The NAM Traffic Analyzer software allows for a shortcut to reduce the time and effort required in setting up a data capture. During typical review of monitor reports, you may come across an entry that you determine requires more in-depth analysis using data capture. Rather than going to the **Capture > Settings** dialog and hoping you remembered all the pertinent information to set up the capture filters, you can simply select the entry in the monitor report table and click the **Capture** button. This action sets up a data capture using the data in the table entry as the filter values. The collection is immediately started and the user is shown the decode screen of the packets captured so far.

Packet Capture and Decode

Custom Capture Filters

Capture > Custom Filters > Capture Filters



Capture Filters Last Modified

↑-- Select a filter then take an action --> **Create** Edit Delete

Select protocol encapsulation and protocol to base filter on. Leave blank if filter is protocol independent.

Enter your data string here. You must enter the hexadecimal value of the data string you want to filter on.

The mask fields (Hex) enable you to define which portions of the data string are relevant for filtering and which portions can be ignored.

The Offset (decimal) and Base options instruct the filter where in the packet to begin searching for the data string.

Status and status masks enable you to search for the status of Ethernet frames that are oversized or undersized or have CRC/alignment errors.

Creating Custom Capture Filters

If the filters that the packet capture settings options do not provide you with enough control over filters, you can create your own filter in the **Capture > Custom Filters > Capture Filters** menu.

Custom filters enable you to search for data patterns found either in the protocol headers or in the data field of the packet. This gives you the ability to read the packet as a single hexadecimal data stream where you can tell the NAM to capture or disregard packets that match the data pattern that you defined in the custom filter options. To use this feature, you need to identify a few things:

- You will need to write the data pattern you are looking for in hexadecimal. Refer to the User Guide for more instructions on hexadecimal and data pattern matching.
- You will also need to tell it where to begin the data pattern search. If you choose absolute, you are telling the filter to beginning looking at the first bit of the packet. If you choose protocol, you are instructing the filter to begin looking at the first bit of the protocol header.
- Status masks enable you to filter on error conditions in Ethernet frames such as oversized or undersized frames or CRC/alignment errors. These are defined by the NAM and you must use values assigned to each of these in order to filter by status.

Defining your own custom filters is a very powerful and complex tool that requires thought and preparation. Refer to the Settings Chapter of the User Guide for more detailed information and instructions on defining custom filters.

Packet Capture and Decode

Decoding Packets

From the **Capture > Buffer** or **Capture > Files** dialogs, select a buffer/File then **Decode**

Decode

Apply filter to limit packets displayed

Traffic Analyzer - Packet Decoder

The screenshot shows the Traffic Analyzer - Packet Decoder interface. At the top, there's a 'Capture1' tab and a 'Packets: 1-1000 of 1381' indicator. Below this is a table of captured packets with columns: Pkt, Time(s), Size, Source, Destination, Protocol, and Info. Packet 1 is highlighted. To the right of the table, there's a 'Display Filter' button and a 'TCP Stream' button. Below the table, there's a detailed view of the selected packet (Packet 1). This view is divided into two panes. The top pane shows a summary of the packet, including the protocol stack (Ethernet II, VLAN, IP, TCP, HTTP) and the data field. The bottom pane shows a hexadecimal dump of the packet data. Callouts point to various parts of the interface: 'From the Capture > Buffer or Capture > Files dialogs, select a buffer/File then Decode' points to the 'Decode' button; 'Apply filter to limit packets displayed' points to the 'Display Filter' button; 'This pane gives summary information for each packet.' points to the packet list; 'This pane gives detailed information about the packet highlighted in the summary section. This section includes Layer 2, 3, and 4 headers and the contents of the data field.' points to the detailed packet view; and 'This pane gives a hexadecimal dump of the packet.' points to the hex dump.

Pkt	Time(s)	Size	Source	Destination	Protocol	Info
1	0.000	422	nmta-core2-6509-NAM	sic-vpn7-26.cisco.com	HTTP	HTTP/1.1 302 Found (text/html)
2	0.027	66	stage-2.cisco.com	54.70.163.166	TCP	2201 > microsoft-ds ISYNI Seq=992379574 Ack=0 Win=16384 Len=0 MSS=1460
3	0.027	66	stage-2.cisco.com	54.70.163.166	TCP	2201 > microsoft-ds ISYNI Seq=992379574 Ack=0 Win=16384 Len=0 MSS=1460
4	0.029	66	stage-2.cisco.com	54.70.163.166	TCP	2201 > microsoft-ds ISYNI Seq=992379574 Ack=0 Win=16384 Len=0 MSS=1460
5	0.074	66	stage-2.cisco.com	160.59.137.88	TCP	2157 > microsoft-ds ISYNI Seq=3869079734 Ack=0 Win=16384 Len=0 MSS=1460
6	0.075	66	stage-2.cisco.com	160.59.137.88	TCP	2157 > microsoft-ds ISYNI Seq=3869079734 Ack=0 Win=16384 Len=0 MSS=1460
7	0.075	66	stage-2.cisco.com	160.59.137.88	TCP	2157 > microsoft-ds ISYNI Seq=3869079734 Ack=0 Win=16384 Len=0 MSS=1460
8	0.077	683	sic-vpn7-26.cisco.com	nmta-core2-6509-NAM...	HTTP	GET /capture/set
9	0.078	683	sic-vpn7-26.cisco.com	nmta-core2-6509-NAM...	HTTP	GET /capture/set
10	0.078	64	nmta-core2-6509-NAM	sic-vpn7-26.cisco.com	TCP	www > 4602 IACK=4602

Packet Details:
Number: 1 - Time: Sep 11, 2006 17:11:10.318 - Packet Length: 422 bytes - Capture Length: 422 bytes
Ethernet II, Src: Cisco Time: Jul 27, 2005 18:26:20.153, Dst: Cisco 31:6e:40 (00:12:da:31:6e:40)
VLAN 802.1Q Virtual LAN
IP Internet Protocol, Src: nmta-core2-6509-NAM.localdomain (192.168.137.82), Dst: Transmission Control Protocol, Src Port: www (80), Dst Port: 4602 (4602), Seq: 1
HTTP Hypertext Transfer Protocol
HTTP/1.1 302 Found
Request Version: HTTP/1.1
Response Code: 302
Date: Mon, 11 Sep 2006 17:11:10 GMT
Server: Apache/1.3.3.6

Hexadecimal Dump:
0000 00 12 da 31 6e 40 00 11 5d 03 b8 00 81 00 00 20 ...ln8..1.....
0010 08 00 45 00 01 94 8a fa 40 00 3f 06 cb 3f c0 a8 ..E.....0.?.?.?
0020 89 52 0a 15 90 1a 00 50 11 fa 5b 7e b7 93 bb c4 ..R.....P...f~....
0030 c0 1a 50 18 41 28 e2 03 00 00 48 54 54 50 2f 31 ..P.A.....HTTP/1

Decoding Packets

To view and filter the results of your data capture, select the buffer to decode from the **Capture > Buffers** dialog, and click **Decode**. The upper portion of the screen shows you summary information for each packet. Fields in this section include:

Pkt—This includes the sequence number assigned by the NAM as it entered the switch.

Time—This is a relative timestamp indicating how much time has elapsed since the capture of the first displayed packet (not the first packet in the buffer). You can also view time by absolute time. Check the User Guide for more information.

Size—This field gives the size of the packet in bytes.

Source—This field gives the address (either Layer 2 or Layer 3) or IP host name of the device transmitting the packet.

Destination—This field gives the address (either Layer 2 or Layer 3) or IP host name of the device receiving the packet.

Protocol—This field gives the highest layer of protocol that the NAM recognizes.

Info—This field gives Information providing more detail about the packet.

The contents in the lower half of the screen provide you with detailed information about the packet you have highlighted in the upper portion of the screen. This detailed information provides you with information in the fields of each protocol header of the packet as well as the data field. You can also see the Layer 2 Ethernet header information as well as portions of the layer 3 IP header information. Use the +/- symbols to the left of each header to view more packet details. The bottom pane displays the hexadecimal dump of the packet, which includes the same information as in the upper portion of the detail window, but written in hexadecimal.

You can also apply a filter on the contents in the frame to refine your view of packets (**Display Filter** button). You can filter by IP or MAC address, or by a plaintext pattern found in packet summary, or you can apply a custom, post-capture filter by choosing the option of your choice from the pull-down list above the Information field.

Packet Capture and Decode

Custom Display Filters

Capture > Custom Filters > Display Filters

If you do not want to filter by protocol, choose ALL from the protocol pull-down list.

If desired, enter addresses as part of the filter definition.

Enter the data string or pattern that you want to filter on. Remember this must be written in hexadecimal.

The Offset and Base options instruct the filter where in the packet to begin searching for the data pattern you defined above.

You can use Boolean logic to define more complex filters.

Creating Custom Display Filters

You can apply the same powerful filter control over captured packets as you can over the capture process by creating your own display filter by selecting the **Capture > Custom Filters > Display Filters** task. You have the same option for searching for data patterns found either in the protocol headers or in the data field of the packet. To use this feature, you need to identify a few things:

- Again, you need to write the data pattern you are looking for in hexadecimal.
- You also need to tell it where to begin the data string search. If you choose absolute, you are telling the filter to begin looking at the first bit of the packet. If you choose protocol, you are instructing the filter to begin looking at the first bit of the protocol header.

Another feature unique to this filter is the option to use Boolean logic to define more complex Decode Filters, using the Filter Expression field. Defining your own custom filters is a very powerful and complex tool that requires thought and preparation. Refer to the Settings chapter of the User Guide for more detailed information and instructions on defining custom filters.

Packet Capture and Decode

Decoding Packets – TCP Stream

The screenshot displays the NAM Traffic Analyzer - Packet Decoder interface. The top section shows a packet capture list with columns for Pkt, Time (s), Size, Source, Destination, Protocol, and Info. A packet is selected, and the 'TCP Stream' button is highlighted. The bottom section shows the decoded TCP stream, including the raw packet data and the decoded HTTP request and response.

Packet Capture List:

Pkt	Time (s)	Size	Source	Destination	Protocol	Info
1	0.000	422	nmb-core2-6509-NAM	sic-von7-26.cisco.com	HTTP	HTTP/1.1 302 Found
2	0.027	86	stage-2.cisco.com	54.70.163.166	TCP	2201 > microso
3	0.027	86	stage-2.cisco.com	54.70.163.166	TCP	2201 > microso
4	0.029	86	stage-2.cisco.com	54.70.163.166	TCP	2201 > microso
5	0.074	86	stage-2.cisco.com	160.59.137.88	TCP	2157 > microso
6	0.075	86	stage-2.cisco.com	160.59.137.88	TCP	2157 > microso
7	0.075	86	stage-2.cisco.com	160.59.137.88	TCP	2157 > microso
8	0.077	883	sic-von7-26.cisco.com	nmb-core2-6509-NAM	HTTP	GET /capture/se
9	0.078	883	sic-von7-26.cisco.com	nmb-core2-6509-NAM	HTTP	GET /capture/se
10	0.078	84	nmb-core2-6509-NAM	sic-von7-26.cisco.com	TCP	www > 4802 (a

Decoded TCP Stream:

```
GET /capture/settings.php?capname=Capture1&refresh=1 HTTP/1.1
Host: 192.168.137.82
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CL
Accept: image/gif, image/x-bitmap, image/jpeg, image/png, application/vnd.ms-excel, applica
Referer: http://192.168.137.82/capture/settings.php
Accept-Language: en-us

21c6
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content
</script>
<script language="JavaScript" SRC="/include/global.js" TYPE="text/javascript"></script>
<div id="overDiv" style="position: absolute; visibility: hidden; z-index: 1;"></div>
<script language="JavaScript" SRC="/include/overlib.js" TYPE="text/javascript"></script>
<script language="JavaScript" SRC="/include/divvalout.js" TYPE="text/javascript"></script>
<script language="JavaScript" SRC="/include/divvalhelp.js" TYPE="text/javascript"></script>
</html>
```

Decoding Packets – TCP Stream

Packet analysis is very beneficial for troubleshooting packet level problems. The NAM offers an additional analysis tool to enhance this process, the TCP Stream tool. To launch, select a TCP packet from the packet decode window, and click the **TCP Stream** button. A new window is opened following that TCP stream through the packet capture providing you with every detail available in the TCP packet including the data.

Packet Capture and Decode

Analyzing Packets

Capture > Files

Storage: Local Disk File Name: Filter 0.01 GB total files

	Name	Size
<input checked="" type="checkbox"/>	Capture2	6.05 MB
<input type="checkbox"/>	Capture1	0.06 MB

Select item(s) then take an action --> **Analyze** Decode Rename/Merge Download

Capture Statistical Analysis
Current Data: as of Mon 11 Sep 2006, 19:20:14 UTC

Capture2.pcap

Packets captured: 32148 Start time: Mon Jun 5 03:22:59 2006
Bytes captured: 8945867 bytes Duration: 0 hours 38 minutes 33 seconds
Avg Packet Size: 278.27 bytes Data Rate: 3867.03 bytes/s (30936.24 bits/s)

From: 0:00:00 To: 0:38:33 Protocol: Host/subnet: Drill-down

Traffic over Time (Granularity: 5 secs)

Protocol Statistics

Protocols	Packets	Bytes
vlan	32148	8945867
ip	32148	8945867
tcp	352	64145
http	40	42755
short	35	38855
unreassembled	2	2644
image-gif	1	384
telnet	14	1076
icmp	1190	123728
ospf	6145	758574
udp	24461	7999420
snap	24428	7996054
short	5534	4834888
data	33	3366

Hosts Statistics

Hosts	Packets	Bytes
192.168.137.105	16270	2373444
192.168.137.82	11166	1319034
192.168.159.2	7715	1744167
224.0.0.5	5822	716684
192.168.159.33	755	99062
192.168.159.42	734	87164
192.168.159.41	737	95750
192.168.159.36	736	87232
192.168.159.37	736	95452
192.168.159.40	736	87556
192.168.159.35	734	87032
192.168.159.38	734	87800
192.168.159.34	1368	172743
10.76.40.84	809	171040

Presents detailed statistical analysis of captured data

- Traffic Rate over selected time period
- List of host and associated traffic
- List of protocols and associated traffic

View more details about a specific time frame, protocol, and/or host/subnet, enter the appropriate data and click Drill Down

Analyzing Packets

The NAM can also provide you with statistical details of any captured file (buffers must be on the NAM local hard drive or a previously defined external drive) providing you with traffic rates and hosts and application stats for a given time period. To launch, go to the **Capture > Files** task. A list of the files stored on the local NAM hard drive are displayed. Use the **Storage** pull down menu to see files stored on one of the defined external drives. Select the file to analyze and click the **Analyze** button. A new window is displayed showing statistics for the entire capture. You can fine tune which statistics are displayed by entering a combination of time, protocol, and/or host and clicking the **Drill-Down** button.

Note(s):

- An additional remote external drive can be configured to expand the data storage capabilities of the NAM. Later in this section, it will be discussed on how to setup the additional storage.

Packet Capture and Decode

Save to NAM Hard Disk (Local Disk)

Two Methods

Capture Settings

☐ Capture to Buffer: Buffer Size (MB): 10 ☐ Wrap when Full

☒ Capture to Disk: File Size (MB): 100 No. Files: 1 ☐ Rotate Files

File Location: Local Disk

Selecting "Capture to Disk > Local Disk" option as the storage option in the Capture Settings

Selecting "No. Files" to be greater than 1, could create multiple files that could be merged into a single file later

You Are Here: [Capture](#) > [Buffers](#)

Capture Buffers

Current Data: as of Wed 08 Jun 2005, 19:30:36 UTC

☒ Auto Refresh

300 MB total buffer memory 300 MB allocated 0 MB available

	Name	Owner	Start Time	Buffer Size	Packets	Status
<input checked="" type="radio"/>	APP_http	LocalMgr	Wed 27 Jul 2005, 06:34:00	10 MB	27110	Locked
<input type="radio"/>	Jeff	LocalMgr	Wed 27 Jul 2005, 18:08:26	10 MB	38076	Locked
<input type="radio"/>	CONVS_192_168_152_134and192_168_159_118	LocalMgr	Thu 28 Jul 2005, 09:54:30	10 MB	40998	Locked
<input type="radio"/>	HOST_171_69_69_84	LocalMgr	Fri 29 Jul 2005, 23:07:39	10 MB	798	Running

Select item(s) then take an action -->

[New Capture](#) [Settings](#) [Decode](#) [Save to File](#) [Delete](#) [Delete All](#)

Selecting the capture from the list of capture buffers and manually saving it to the NAM Hard Disk

Save to NAM Hard Disk

By default, the NAM stores the captured packets in a buffer in RAM. Saving buffers to the NAM's local hard drive allows you to keep the traffic filtered and capture for analysis at a later time as well as free up memory for other capture buffers or NAM monitoring.

There are basically two ways to store buffers to the NAM's local hard drive.

1. The first method is to simply select a buffer from the [Capture > Buffers](#) list and click [Save to File](#).
2. The second method is to configure the NAM to Capture to Disk. This configuration option was described earlier under "Capture Settings" topic. Note that if the [No. Files](#) option is greater than 1, multiple files will be created on the hard drive.

Upcoming in this section, it will be discussed on how to merge multiple files on the local NAM hard drive or a defined external storage device.

Packet Capture and Decode

Additional Remote Data Storage (Optional)

Extend the NAM's data capture storage capability, by defining remote storage locations

Before using a remote disk to store data captures, use the **Admin > System > Capture Data Storage** task to first define it

A remote data storage can be of either type:

- NFS
- iSCSI

Additional Remote Data Storage (Optional)

For flexibility and increased storage, the NAM can also store the packets captured on a remote disk.

To use the remote disk option, configure the NAM with details about the remote disk, using the **Admin > System > Capture Data Storage** task.

The remote storage server can be of either type: NFS or iSCSI.

Packet Capture and Decode

Defining Remote Data Storage (NFS)

CISCO SYSTEMS NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Users System Diagnostics

You Are Here: Admin > System > Capture Data Storage

Capture Data Storage

Type	Name	Server Address	NFS Directory / iSCSI Target Name	Free Storage
Select an entry then take an action				
Create NFS				Create iSCSI
Edit				

New NFS Storage

Name: remoteDC

Server: pvm-1.cisco.com

Directory: /export/nam

Basic NFS Options

Protocol: UDP NFS version: 3

Timeout (seconds): 0.2 Retries: 2

Advance NFS Options: soft,timeo=2,udp,nfsvers=3,retrans=2

Submit Reset Cancel

NOTE: The NFS server must be able to grant access to the NAM in order to write to the disk (see notes on procedure)

Defining Remote Data Storage (NFS)

To use a NFS remote disk, click the **Create NFS** button to define it. Provide a name for the disk (in order to identify it in the NAM user interface), enter the hostname of the server that has the remote disk, and provide the directory as to where the capture files should be located.

Note(s):

- The NFS server must be configured to grant read and write access to the NAM in order for the NAM to be able to store capture files on it. The following example shows how to set up an NFS directory (/home/SomeUserName) on a Linux server for a NAM (at IP address 1.1.1.2) to store capture data.
 - Locate a UID that has read and write access to the target NFS directory.
 - For example, if the target NFS directory is /home/SomeUserName, open the /etc/passwd file and search for a user entry that contains something like the following:
SomeUserName:x:503:503::/home/SomeUserName:/bin/tcsh
 - In this example, the UID is 503.
 - Edit the /etc/exports file and add a line like the following:
/home/SomeUserName 1.1.1.2/255.255.255.255(rw,all_squash,anonuid=503)
 - Activate the change: type: /usr/bin/exportfs -a
- If the NFS directory contains subdirectories that are not writable by the NAM, these subdirectories will not be listed in NAM capture screens.

Packet Capture and Decode

Defining Remote Data Storage (iSCSI)

CISCO SYSTEMS NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Users System Diagnostics

You Are Here: Admin > System > Capture Data Storage

Capture Data Storage

Capture Data Storage Table

Type	Name	Server Address	NFS Directory / iSCSI Target Name	Free Storage
Select an entry then take an action -->				
Create NFS Create iSCSI Edit				

New iSCSI Storage

Name:

Server:

Target Name:

Format Disk:

☐ Format a new partition

☒ Use existing partition:

[Submit](#) [Reset](#) [Cancel](#)

NOTE: Before the new iSCSI storage entry takes effect, you must reboot the NAM system to load the drivers

NAM / Traffic Analyzer v3.5 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-167

Defining Remote Data Storage (iSCSI)

To use a remote iSCSI disk that is located on an iSCSI server, click the **Create iSCSI** button to define it. Provide a name for the disk (in order to identify it in the NAM user interface), enter the hostname of the iSCSI server that has the remote disk, and provide the iSCSI target name configured on the remote server.

Check **Format a new partition** to cause the NAM to format the iSCSI target into a single Linux partition.

Check **Use existing partition#** when the remote iSCSI target disk has already been formatted and has a partition table.

Notes:

- Before the NAM can recognize the configured iSCSI device, the NAM must be restarted so that it can load the device drivers.

Packet Capture and Decode

Managing Capture Files

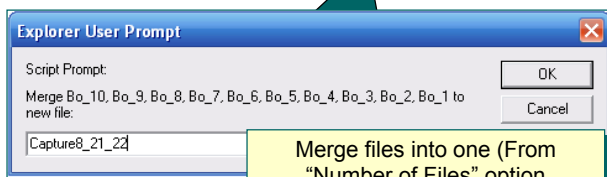
Capture > Files

Storage	File Name	Filter	0.00 GB total file size	2.1 GB available disk space
	Name	Size	Date	
<input type="checkbox"/>	Arg_1	2.35 MB	Tue 11 Jul 2006, 19:04:52	
<input type="checkbox"/>	Capture2	7.03 MB	Mon 26 Jun 2006, 20:07:50	
<input checked="" type="checkbox"/>	Bo_10	6.18 MB	Sat 22 Apr 2006, 05:25:03	
<input checked="" type="checkbox"/>	Bo_9	6.15 MB	Sat 22 Apr 2006, 07:07:51	
<input checked="" type="checkbox"/>	Bo_8	6.18 MB	Sat 22 Apr 2006, 05:03:06	
<input checked="" type="checkbox"/>	Bo_7	5.84 MB	Sat 22 Apr 2006, 02:54:42	
<input checked="" type="checkbox"/>	Bo_6	6 MB	Sat 22 Apr 2006, 01:19:14	
<input checked="" type="checkbox"/>	Bo_5	6.12 MB	Fri 21 Apr 2006, 23:45:19	
<input checked="" type="checkbox"/>	Bo_4	6.1 MB	Fri 21 Apr 2006, 22:33:33	
<input checked="" type="checkbox"/>	Bo_3	6.08 MB	Fri 21 Apr 2006, 21:04:13	
<input checked="" type="checkbox"/>	Bo_2	6.14 MB	Fri 21 Apr 2006, 19:39:04	
<input checked="" type="checkbox"/>	Bo_1	6.14 MB	Fri 21 Apr 2006, 18:29:11	
<input type="checkbox"/>	APP_snmp	8.26 MB	Tue 18 Apr 2006, 22:37:03	
<input type="checkbox"/>	Automatic_Capture	0.7 MB	Thu 06 Apr 2006, 03:43:08	

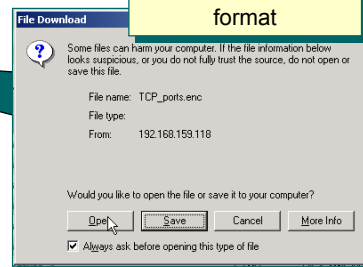
← Select item(s) then take an action --> Analyze Decode Rename Merge Download Delete Delete All

Select capture files on NAM hard disk (Local) or Remote Disk

Download selected file to your computer in Sniffer .enc file format



Merge files into one (From "Number of Files" option)



Managing Capture Files

Like the buffers in NAM memory, it is important to be able to manage the capture files stored on either the NAM hard drive or any defined external storage devices. Several tasks can be performed on these files using the **Capture > Files** task, which will list all files found on the NAM hard drive.

Decode – Select the desired file and decode it (just like decoding buffers).

Analyze – Provide traffic, protocol, and host rates over time for the capture file

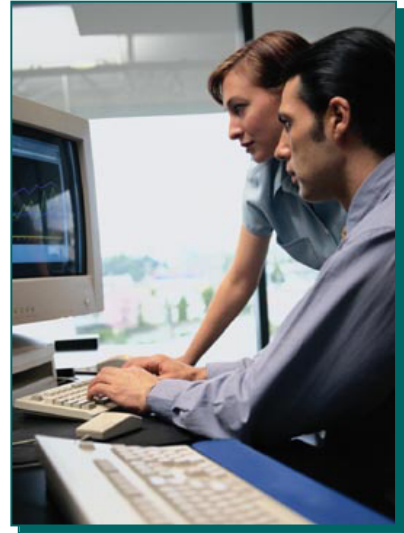
Merge – Select multiple files and merge them into a single file.

Download - Save a selected file to your client machine in the .enc Network General Sniffer format.

Delete & Delete All – delete one or all the files from the NAM hard drive.

Product Features - Summary

- **Flexible Monitoring**
 - LAN/WAN
 - SPAN/RSPAN/VACL
 - NDE
- **Comprehensive Visibility**
 - Application
 - Host
 - Conversation
 - Voice
 - DiffServ
 - VLANs
 - MPLS Tags
- **Historical Trend Reports**
- **Packet Capture and Decode**



Feature Summary

We have covered all of the ground that we set out to do with the road map for implementing the NAM in your environment, and in the process we covered almost all the features available to you with the NAM and the embedded Traffic Analyzer software.

Now let's look at some scenarios that apply the NAM and its feature set to solving real-world problems.

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATIONSM

Thank You!

Continue on to Chapter 3 to learn how to use the NAMs through a series of scenarios.



NAM Usage Scenarios

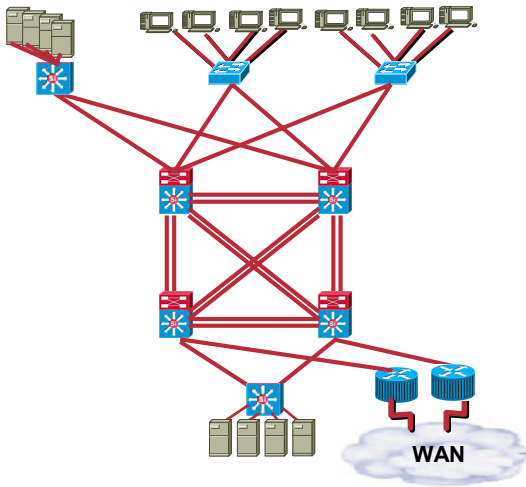
Chapter 3

- **Cisco Network Analysis Modules (NAM)
NAM-1, NAM-2, and the NM-NAM**
- **Cisco NAM Traffic Analyzer Software v3.5**

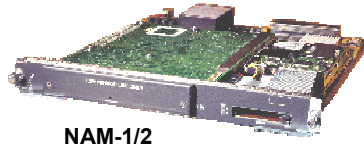


Chapter 3 Outline

NAM Scenarios



- Performance/Troubleshooting (NAM-1/2)
- Performance/Troubleshooting (NM-NAM)
- QoS Monitoring (Using DiffServ and ART)
- VoIP Monitoring
- Trend Analysis



NAM-1/2



NM-NAM

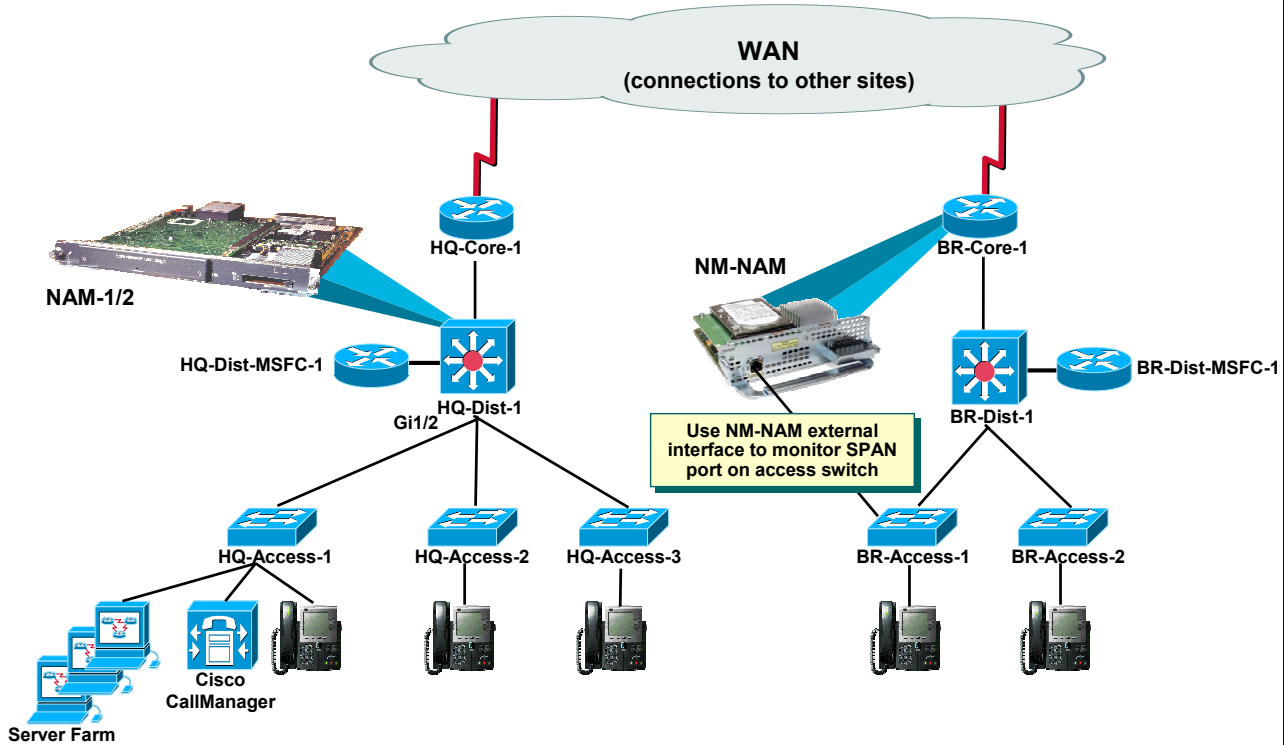
Chapter 3 Outline

This chapter explores several scenarios to illustrate how you can use the various Network Analysis Modules (NAM) to gain visibility into your network. These scenarios will help you understand how to configure and use the NAM to solve problems as or before they arise.

In general, the NAM and its embedded Traffic Analyzer software can help you quickly determine how various services on your network are performing, as well as, the applications and users that consume services and resources on your network. By going through these scenarios you will learn how to configure the NAM to collect the data you want, and how to use its embedded Traffic Analyzer software to view service and application performance and the various levels of traffic statistics that the NAM offers. But first, let's look at the network environment that we will use in these scenarios.

Network Overview

Q-Bits International



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-3

Network Overview - Q-Bits International

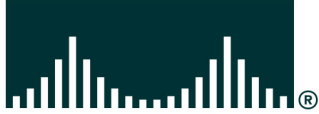
Q-Bits International has recently adopted Cisco's strategy for converging voice, video, and data onto a single network infrastructure using the Cisco AVVID (Architecture for Voice, Video and Integrated Data). Using Cisco AVVID, Q-Bits has converged its two networks—its data network and its proprietary voice private branch exchange (PBX) system—onto an open, standards-based network infrastructure.

Dean Jones, a lead network engineer for Q-Bits, has been tasked with verifying the policies behind the network redesign as well as the day-to-day performance of the new network. He has decided that he needs visibility into the traffic traversing the network to determine whether or not the rollout has been successful. He knows that he needs the ability to determine the utilization of the network, but he also wants to know which applications and hosts are using network resources. In addition, he needs to verify the performance of voice applications and the new QoS implementation (using Differentiated Services). In short, he needs to verify that the network has been designed correctly and configured to meet defined policies and requirements. He has decided to deploy a single NAM card (NAM-1 or NAM-2) in the company headquarters distribution switch and a branch NAM (NM-NAM) in the core router at the branch facility to help assess the network performance.

Dean knows that with the one NAM card at each site, he can begin to analyze traffic to determine whether or not the network meets policy and performance requirements.

This page intentionally left blank.

CISCO SYSTEMS



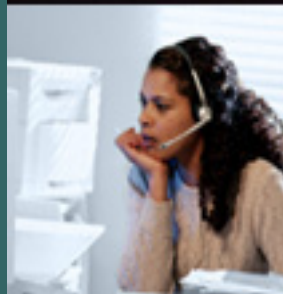
Performance/Troubleshooting (NAM-1/2)

Performance/Troubleshooting
(NM-NAM)

QoS Monitoring

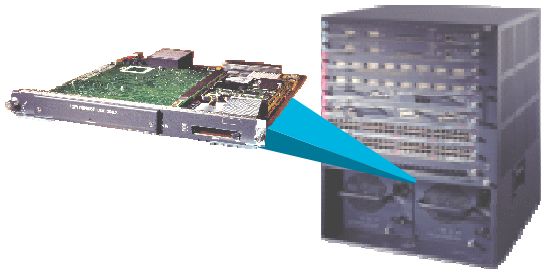
VoIP Monitoring

Trend Analysis



Scenario 1

Performance/Troubleshooting (NAM-1/2)



- NAM Access
- Port Utilization
- Port Spanning
- Traffic Overview
- Unwanted Traffic Users

Scenario 1 - Performance/Troubleshooting NAM-1/2

After Dean installs and configures the Catalyst 6500 series NAM module, he is ready to see if the new network is performing as expected. Because the switch with the new NAM is central to most traffic flowing through the Headquarters' network, Dean should be able to determine very quickly how the network is performing. To do so, Dean first looks at the ports on the switch to get a snapshot of their current utilization. From there, he can drill down for more detailed views of traffic for any port or virtual LAN (VLAN). As you will see, Dean discovers some unwanted traffic, and he uses the NAM to find out who is generating it.

Note: Notation used for task selection will be in the form of **Tab > Option > Sub-Option**.

Scenario 1

Accessing the NAM

The screenshot shows a web browser window titled "nm1tg-hq-core-6506-nam - Login - NAM Traffic Analyzer - Microsoft Internet ...". The address bar contains "http://192.168.159.118/auth/login.php", which is circled in red. A yellow callout box points to this address bar with the text: "Enter user account information created during the installation of the NAM".

The login screen displays a "Please login:" section with fields for "Name:" and "Password:", and a "Login" button. A red dashed box highlights the "Login" button, with a red arrow pointing to the "System Overview" section of the next screen.

The "System Overview" screen shows the "System Resources" menu on the left and a "System Overview" table on the right. The table contains the following data:

System Overview		
Date:	Wed 13 Sep 2006, 18:23:18 UTC	
Hostname:	nm1tg-core2-6509-NAM.localdomain	
IP Address:	192.168.137.82	
System Uptime:	64 days, 21 hours, 36 minutes	
CPU Utilization:	2.5%	
Memory Utilization:	36%	
Disk Usage:	Partitions	Total
	Root	3.94 G
	Config	1,007.87 M
	Data	3.29 G

A yellow callout box points to the "System Overview" section with the text: "NAM Performance Metrics".

Accessing the NAM

Dean can access the embedded web server and Traffic Analyzer software in the NAM with his web browser and the IP address or host name of the NAM as the URL; for example, `http://192.168.159.118`. However, if Dean had assigned a TCP port number other than 80 during configuration, then he would need to append that port number to the end of the URL and use a colon to separate the port number from the address or host name (that is, `http://192.168.159.118:88`).

After Dean enters the URL for his NAM, he is presented with the Traffic Analyzer login screen. He logs into the NAM server using the account information that he defined during installation (see Chapter 4 for more details) and clicks the **Login** button. The Traffic Analyzer authenticates his login information and displays the *System Resources* metrics. Dean reviews the System Resources metrics to ensure that the NAM has sufficient memory and CPU to accommodate his monitoring tasks because he knows that lack of memory or CPU could mean that the NAM might inaccurately collect and report statistics. If resource utilization rises too high, he knows to reduce the number of monitoring tasks he has configured to relieve the performance burden on the NAM.

At this time, Dean could create additional user accounts with specific access privileges. To create new users, Dean performs the following steps:

- Step 1. Select the **Admin** tab, if not already selected.
- Step 2. Select the **Users** option located under the set of tabs displaying NAM functions. A new menu of options is displayed on the left side. Ensure that *Local Database* is selected (select TACACS+ if using TACACS+ for authentication). A list of current users is displayed.
- Step 3. Click **Create**. The *User Information* dialog is displayed.
- Step 4. Enter user account name, password, and privileges.
- Step 5. Click **Submit** to create the new user.

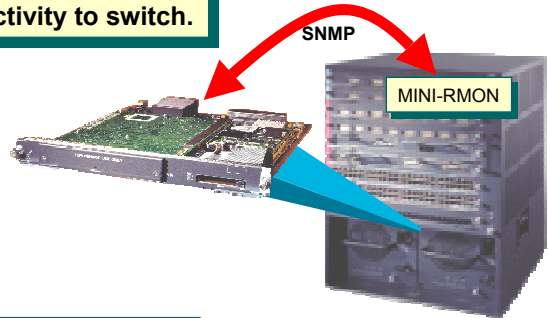
Scenario 1

Setting Switch Parameters

Setup > Switch Parameters > Switch Information

Switch Information	
Performing SNMP test from NAM (192.168.159.118) to switch (192.168.159.117)	
Name:	nmtg-hq-core-6506
Hardware:	Cisco Systems Catalyst 6500 6-slot Chassis System
Supervisor Software Version:	IOS Version 12.2(14)SX1
System Uptime:	20 days, 0 hours, 06 minutes
Location:	N/A
Contact:	N/A
SNMP read from switch:	OK
SNMP write to switch:	OK
Mini-RMON on switch:	Available
NBAR on switch:	Unavailable
VLAN Traffic Statistics on supervisor:	Available
NetFlow Status:	Configured to NAM 172.20.111.163 on port 9991

The NAM SNMP to retrieve Mini-RMON stats. Verify NAM SNMP connectivity to switch.



Setup > Switch Parameters > Port Stats

Port Stats (Mini-Rmon)
Current Status: Enabled
The NAM is currently able to provide Port Stats with this configuration. No further action is necessary.
<input type="button" value="Details"/> <input type="button" value="Save"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/>

Enable/Verify Mini-RMON is enabled on Switch

Setting Switch Parameters

The first thing Dean wants to check is the utilization for every port that supports workgroup access switches. Port statistics are collected and stored in the mini-RMON Management Information Base (MIB) on the switch itself. In mini-RMON, only a few of the RMON groups are collected: statistics, history, alarms, and events. For the NAM to retrieve and display statistics stored on the switch, it must make a Simple Network Management Protocol (SNMP) query to the switch. Use the following steps to ensure SNMP connectivity between the NAM and the host switch, and to enable/verify that mini-RMON is enabled on the switch:

- Step 1. Click the **Setup** tab. A set of six setup options are displayed in the content window directly under the tabs. Note that the color of the selected tab (Setup in this case) matches the bar directly underneath, which displays the options for the tab selected. The text of the selected tab is black. All unselected tabs are darker in color with white text.
- Step 2. Click on the **Switch Parameters** option. The Switch Parameter text underneath the tab turns black to indicate it is selected. A sub-menu is displayed on the left-side of the screen with further options for *Setup > Switch Parameters*.
- Step 3. Click **Switch Information**. The *Switch Information* dialog is displayed. Verify that the NAM has SNMP connectivity to the switch.
- Step 4. From the sub-menu, click **Port Stats (Mini-RMON)**. The *Port Stats (Mini-RMON)* dialog is displayed. Verify that Mini-RMON is enabled. If not, select enable. (If using a Cat IOS device, then click **Save** for the changes to be written to the start-up config).
- Step 5. To see details of which ports are enabled for mini-RMON, click **Details**.

Scenario 1

Switch Port Utilization

Monitor > Switch > Port Stats

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Count Types: Traffic Rates Port Name: Filter Clear

Showing 1-5 of 5 records

#	Port Name	Utilization %	Bytes/s	Packets/s	Broadcast/s	Multicast/s	Errors/s
1.	Fa4/1	0.00	1,073.49	14%	5.08	0.00	0.35
2.	Gi1/2	0.00	5,657.06	76%	47.25	3.50	18.20
3.	Gi1/3	0.00	361.36	5%	2.30	0.00	0.26
4.	Gi3/2	0.00	339.39	5%	1.42	0.00	0.18
5.	Gi1/1	0.00	46.64	1%	0.39	0.00	0.25

Rows per page: 50 Units: Bytes/s Go to page: 1 of 1 Go

Select an item then take an action --> Details Real-Time Report

Check port status for any indication of problems.

Switch Port Utilization

Dean can now look at the utilization of each of the Cisco Catalyst® Switch ports that host the NAM card.

Step 1. Click **Monitor > Switch > Port Stats**. The *Port Stats* data screen is displayed.

Most of the monitor views offer three perspectives—Current Rates, TopN Chart, and Cumulative Data. These can be chosen by clicking the radio buttons at the top of the data table. By default, the Current Rates table is displayed first. This table provides statistics for traffic collected during the last refresh cycle only. The *TopN* chart provides a list of ports ranked by volume for data during the last refresh cycle only, and the *Cumulative Data* table provides absolute values for data collected since the min-RMON counters were last cleared.

The refresh cycle can be modified by selecting *Setup > Preferences*, changing the *Refresh Interval*, and clicking *Apply*. If the *Auto Refresh* check box is selected on any data screen, the tables and charts will be refreshed as new data is collected.

Using these views, Dean happily notes that all ports on his switch are barely utilized. This confirms the bandwidth predictions Q-Bits used to design its network. If any abnormally high utilization or error conditions had existed, Dean could use them to help determine where to begin looking for the causes. To drill down, Dean can SPAN any port or combination of ports to the NAM for complete traffic analysis of the data traversing that port.

Because nothing looks out of the ordinary here, Dean decides to SPAN port Gi1/2, which connects to the server farm workgroup access switch, to look at traffic flowing to/from the server farm.

Scenario 1

SPAN Traffic To/From Server Farm

Setup > Data Sources > SPAN

Create SPAN Session

SPAN Type: ☒ Switch Port ☐ VLAN ☐ EtherChannel ☐ RSPAN VLAN

Switch Module: Module 1: 8 ports (WS-X6408-GBIC)

SPAN Traffic Direction: ☐ Rx ☐ Tx ☒ Both

Available Sources:

- 1/1
- 1/2
- 1/3
- 1/4
- 1/5
- 1/6
- 1/7
- 1/8

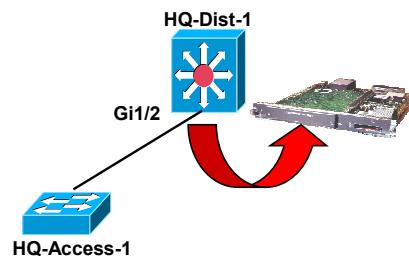
Add Remove Remove All

Selected Sources:

- 1/2 (Both)

Submit

1. Select SPAN Type.
2. Select Switch Module if port SPAN.
3. Select SPAN direction.
4. Select Source.
5. Click **Add**.
6. Repeat steps 4 and 5 if necessary.



SPAN Traffic To/From Server Farm

To use the Switched Port Analyzer (SPAN) on traffic to and from the server farm (port Gi1/2 on distribution switch), perform the following:

- Step 1. Click **Setup > Data Sources > SPAN**. The Active SPAN Sessions dialog is displayed listing the current SPAN session if any.
- Step 2. Click the **Create** button. The Create Span Sessions data screen is displayed.
- Step 3. Select **Switch Port** as the SPAN Type.
- Step 4. From the Switch Module pull-down list, select **Module 1**.
- Step 5. Select **Both** as the SPAN Traffic Direction.
- Step 7. Highlight port 1/2 from the Available Sources list and click **Add**. Port 1/2 moves into the Selected Sources list.
- Step 8. Click **Submit** to make this SPAN session active.

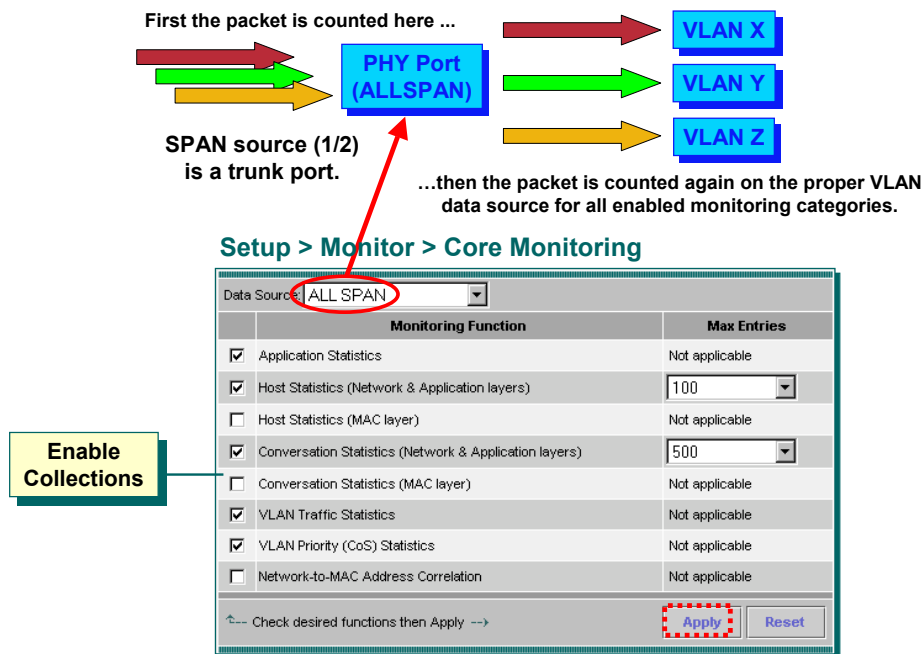
All traffic either received or transmitted by port 1/2 is now being mirrored (copied) to the NAM. However, before any statistics are actually collected, Dean must enable collections on the Traffic Analyzer for the types of monitoring that he wants to perform.

Note: Dean is using a Cisco Catalyst 6500 Series NAM-1 with a single data port known as port slot/3. If you are using a NAM-2, an additional step to creating the SPAN session would be to select the data port. On the NAM-2, the data ports are known as slot/7 and slot/8.

Note: If all data ports are currently configured for SPAN or VACL, then you must first delete the session before creating a new one. If the session is not deleted, you will be asked if you wish to replace the existing session.

Scenario 1

Configure Core Monitoring (ALLSPAN)



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-11

Configure Core Monitoring

The Traffic Analyzer collects and reports data for two types of data sources. The first is an aggregated data source which includes the ALLSPAN data source (and DATAPORT1/2 data source if using a NAM-2). The ALLSPAN aggregation includes a counting of all packets mirrored to the data ports of the NAM by either SPAN or VACL. The second data source type includes the individual VLANs, where every mirrored packet is assigned to and counted in the VLAN that it participates in. In the case of a trunk port, ALLSPAN provides statistics for all traffic traversing the port, regardless of its membership in a VLAN. It is important to understand this because ALLSPAN can report confusing statistics when the NAM is configured for more than one SPAN source. However, monitoring for either or both of these two data sources (ALLSPAN or VLAN) must be configured before the NAM will collect or report data for these data sources. Note too that changing a SPAN source does not change the data source that the NAM is configured to collect for. NetFlow Data Export (NDE) data sources must also be enabled for collection to occur.

To begin monitoring activities, Dean chooses to enable monitoring on the ALLSPAN entity. This gives Dean an overall view of VLAN traffic to see if he needs to drill down into any particular VLAN.

- Step 1. Click **Setup > Monitor > Core Monitoring**. The Core Monitoring Functions dialog is displayed.
- Step 2. The pull-down Data Sources list displays all VLANs known to this switch, as well as, an ALLSPAN entry. Just because a VLAN is listed here does not mean that it has been observed in the SPAN source. Turning on VLAN traffic statistics for ALLSPAN and then viewing VLAN statistic will show which VLANs have been observed in the SPAN sources. If fact, that is what Dean is about to do. Select **ALLSPAN** from the Data Sources pull-down menu.
- Step 3. Enable desired monitoring functions (application, network host, network conversations, VLAN statistics) and click **Apply**.

The NAM now begins collecting these statistics for all traffic on port Gi1/2 (SPAN source).

Note: Because Dean did not enable a specific VLAN for collection, the NAM is not yet collecting data based on individual VLANs.

Scenario 1

VLAN Traffic Statistics

Monitor > VLAN > Traffic Statistics

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source: ALL SPAN

Showing 1-6 of 6 records

#	VLAN ID	Packets/s	Bytes/s	Non-Unicast Pkts/s	Non-Unicast Bytes/s
1	1	1.10	1%	90.08	1.10
2	100	71.27	95%	8,276.23	36.60
3	130	58.00	84%	7,781.33	31.30
4	1014	0.13	<1%	22.90	0.13
5	1015	1.53	2%	179.75	0.13
6	1018	0.13	<1%	10.13	0.13

Rows per page: 10 Units: Bytes/s Go to page: 1 of 1 Go

Select an item then take an action --> Report

Unexpected High Traffic Level.

Who is using this bandwidth?

VLAN Traffic Statistics

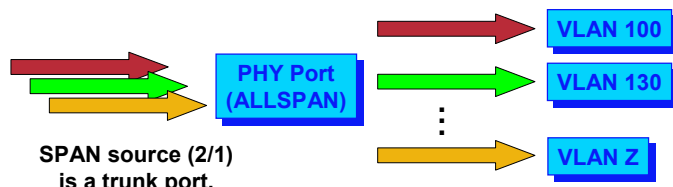
Dean now wants to see which VLANs are passing traffic to and from the server farm and how much.

Step 1. Click **Monitor > VLAN > Traffic Statistics**. The VLAN Traffic Statistics report is displayed.

Dean expects to see most of the traffic to and from the servers on VLAN 100. What he did not expect to see was such a high volume of traffic on VLAN 130. Dean decides to drill down into the details of VLAN 130 to see who is creating this unexpected traffic.

Scenario 1

Configure Core Monitoring for VLAN 130



Enable statistics collection for traffic in VLAN 130.

Setup > Monitor > Core Monitoring

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	100
<input type="checkbox"/> Host Statistics (MAC layer)	Not applicable
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	500
<input type="checkbox"/> Conversation Statistics (MAC layer)	Not applicable
<input checked="" type="checkbox"/> VLAN Priority (CoS) Statistics	Not applicable
<input type="checkbox"/> Network-to-MAC Address Correlation	Not applicable

Check desired functions then Apply -->

Apply Reset

Configure Core Monitoring for VLAN 130

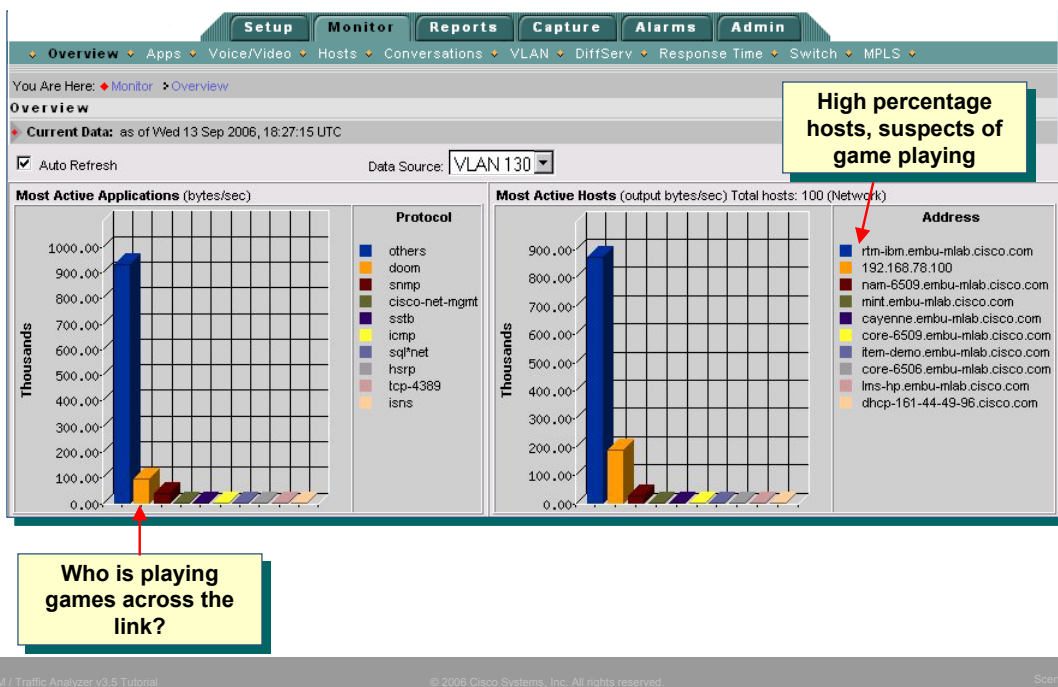
Previously, Dean enabled monitoring functions on the ALLSPAN data source for port Gi1/2, his SPAN source. Now he wants to enable various monitoring functions just for the VLAN 130 portion of port Gi1/2 traffic. To do so, all Dean needs to do to enable monitoring for VLAN 130 is to follow the same steps he used to configure ALLSPAN, except this time he will choose VLAN 130 as his data source rather than ALLSPAN:

- Step 1. Click **Setup > Monitor > Core Monitoring**. The Core Monitoring Functions screen is displayed.
- Step 2. Select **VLAN 130** from the Data Sources pull-down menu.
- Step 3. Enable desired monitoring functions (application, network host, network conversations, VLAN statistics) and click **Apply**.

Dean will now be able to drill down into the traffic statistics on VLAN 130 to determine what and who is using the bandwidth. Also notice that enabling monitoring for VLAN 130 does not disable monitoring for the ALLSPAN data source because the NAM supports monitoring multiple data sources.

Scenario 1

Traffic Overview VLAN 130



Traffic Overview VLAN 130

Dean uses the traffic overview feature of the NAM to get a quick look at what is happening on VLAN 130.

Step 1. Click **Monitor > Overview**. The Overview data screen is displayed.

Step 2. Select **VLAN 130** from the Data Source pull-down menu to display an overview of VLAN 130 traffic. Notice that the only data sources that are available in the list are the VLANs that Dean enabled monitoring for. If Dean had enabled monitoring for VLANs that are not present in his SPAN source, they will be listed here because he enabled monitoring for them, but no data will be displayed because they do not exist in the SPAN source.

Dean immediately notices suspicious activity. First, he observes that the second most active application on his SPAN source is Doom. Then he looks at the most active hosts to determine who might be playing Doom. He identifies two potential suspects and determines that he needs to investigate further. But Dean also notices a lot of “other” traffic (traffic using TCP or User Datagram Protocol [UDP] ports that are not well known – grouped as “other” after the configured number of auto-discovered unknown apps are found). He decides that he must deal with the gamers first, but he also makes a note of this other traffic because he knows that he can configure the NAM to identify and collect statistics for this other traffic.

Note: Dean would have also seen the Doom traffic by looking at the overview of ALLSPAN traffic because VLAN 130 is a subset of ALLSPAN. But by looking just at VLAN 130 statistics, Dean is able to localize the traffic. This could be useful if a certain application is allowed on one VLAN but not another. Then the application traffic would be seen at the ALLSPAN level, but hopefully not at the VLAN level it is prohibited on.

Scenario 1

Apps and App Consumers on VLAN 130

Monitor > Apps > Individual Applications

Current Rates TopN Chart Cumulative Data

Data Source: **VLAN 130** Protocol: Filter Clear

Showing 1-5 of 165 records

#	Protocol	Packets/s	Bytes/s
<input type="radio"/> 1.	others	2009.60	949973.12
<input checked="" type="radio"/> 2.	doom	1054.13	96980.27
<input type="radio"/> 3.	http	98.13	31102.78
<input type="radio"/> 4.	snmp	25.57	4901.67
<input type="radio"/> 5.	cisco-net-mgmt	5.50	1814.83

Rows per page: 5 Go to page: 1 of 33 Go

Select an item then take an action--> Details Capture Real-Time Report

Simply click on an application to see all users of that application.

Hosts using w-ether2.ip.tcp.doom

Host	In Pkts	Out Pkts	In Bytes	Out Bytes
rtn-ibm.embu-mlab.cisco.com	42973621	25784176	3747300014	2578417752
192.168.78.100	25784231	42973713	2578423222	3747308000

Close

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-15

Apps and App Consumers on VLAN130

Now that Dean knows that there is some suspect application traffic on VLAN 130, he uses NAM monitor reports to quickly find the consumers. Dean starts by looking at the applications present in VLAN 130, finding Doom, and drilling down to see the hosts sending and receiving Doom traffic.

- Step 1. Click **Monitor > Apps > Individual Applications**. The Applications report is displayed.
- Step 2. Select **VLAN 130** from the Data Source pull-down menu to display the Applications seen in VLAN 130 traffic.
- Step 3. Find the Doom entry and either click on the Doom text, or select the radio button to the left of the Doom entry and click the **Details** button. A report detailing all the hosts currently sending or receiving Doom traffic is displayed.

Dean can now go and talk to these users and have them stop if he desires. Let's look at some other NAM monitor reports that can give us some additional information about these hosts and their network usage.

Scenario 1

Host View VLAN 130

Zoom in on one of the reported hosts to view details about application usage and conversations

See next page

#	Address	Via	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	Non-Unicast/s
1.	lzo-dan-lan-vlan1-dhcp16.cisco.com	ip	2041.00	2087.00	1471769.00	255755.00	0.00
2.	rtn-lbm-embu-mlab.cisco.com	ip	1779.88	1300.62	192199.54	877920.40	0.01
3.	192.168.78.100	ip	1299.64	1778.96	877610.42	190922.85	0.00
4.	serv-4000-embu-mlab.cisco.com	ip	769.00	770.00	96385.00	95849.00	0.00
5.	lms-lbm-embu-mlab.cisco.com	ip	18.32	18.59	2109.86	2200.84	0.18

Host View VLAN 130

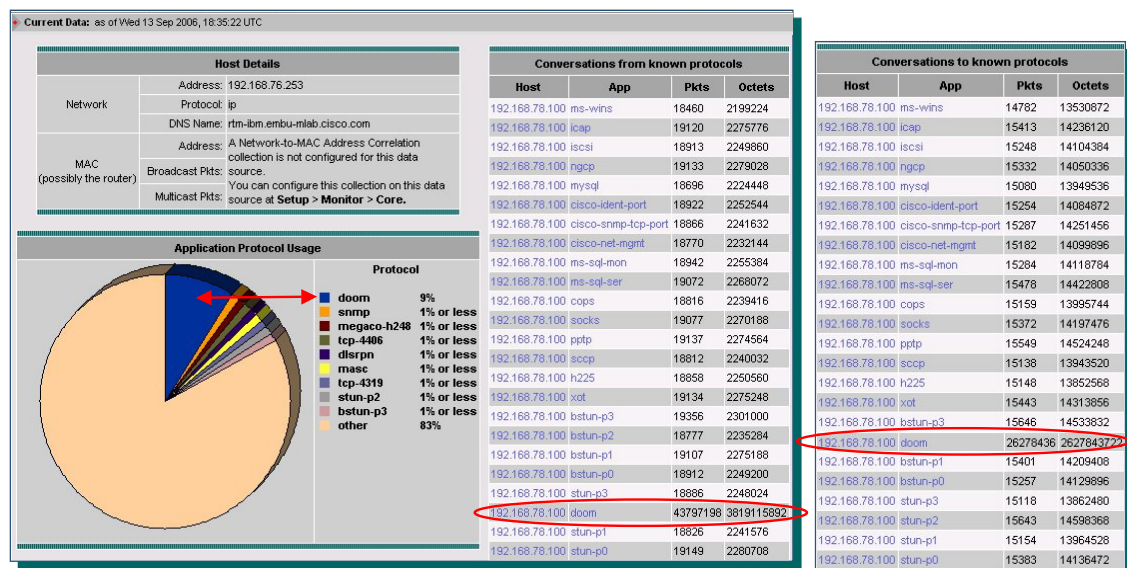
Now that Dean knows which hosts are playing Doom, he wants to determine what other network activities they are involved in. He can do this by looking at all hosts in VLAN 130 and drilling down by host to see application usage and conversations.

- Step 1. Click **Monitor > Hosts > Network Hosts**. The Network Hosts report is displayed.
- Step 3. Select **VLAN 130** from the Data Source pull-down menu to display all hosts sending traffic on VLAN 130.
- Step 4. Choose a sort criteria. Dean clicks on the **In Packets/s** column.

Dean is presented with the users by packet rate on VLAN 130 on SPAN source port Gi1/2. Drilling down into the details of the high-volume users is always a good place to start looking for the source of trouble on the network. This is done by simply clicking on the desired host in the list, or by selecting the radio button to the left of the host entry and clicking the **Details** button. See next page for resulting report.

Scenario 1

Host Zoom



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-17

Host Zoom

Dean drills down on one of the hosts reported as playing Doom and is presented with a wealth of information about its activities. Looking at the Application Protocol Usage chart, Dean quickly sees all applications this host is using, and a listing of conversations to and from each application. If Dean chooses to stop the game, he can verify that the game has been shut down by selecting **Monitor > Apps > Individual Applications** and using **VLAN 130** as the data source to see if any Doom traffic still exists. Before doing this Dean will trend the traffic to determine its impact (see Scenario 5).

This page intentionally left blank.

CISCO SYSTEMS



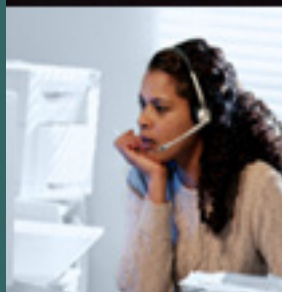
Performance/Troubleshooting
(NAM-1/2)

Performance/Troubleshooting (NM-NAM)

QoS Monitoring

VoIP Monitoring

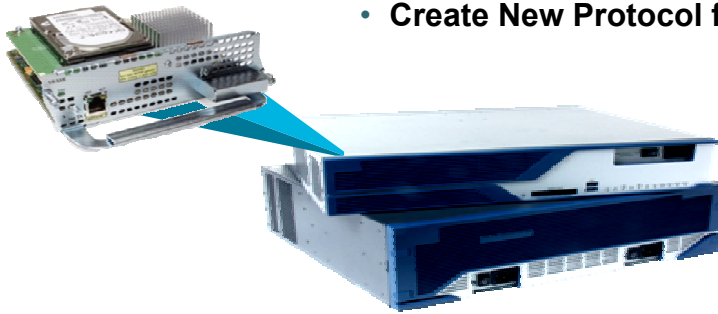
Trend Analysis



Scenario 2

Performance/Troubleshooting (NM-NAM)

- **NAM Access**
- **Interface Utilization**
- **WAN Interface Monitoring**
- **Host Monitor**
- **Packet Capture to Classify Traffic**
- **Create New Protocol for Monitoring**



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-20

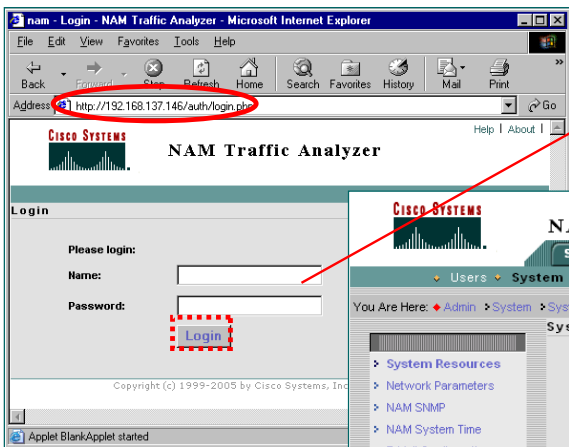
Scenario 2 - Performance/Troubleshooting NM-NAM

The branch office was recently opened and is expected to send lots of proprietary application traffic back to headquarters. Dean has installed a branch router NAM (NM-NAM) in the branch office core router connecting the branch office to the WAN. DEAN wants to configure the NM-NAM to monitor WAN traffic to understand how much of the WAN link is being utilized by the proprietary application.

Note: Notation used for task selection will be in the form of **Tab > Option > Sub-Option**.

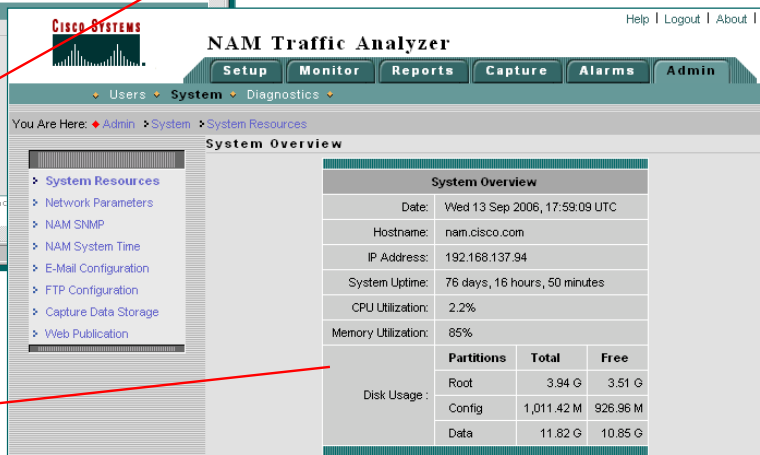
Scenario 2

Accessing the NM-NAM



NM-NAM software is the same as the NAM-1/2 software with a few minor differences, hence, access is the same.

NAM Performance Metrics



Accessing the NAM

Dean accesses the NM-NAM in exactly the same manner as he previously accessed the Catalyst 6500 series NAM by simply entering the IP address assigned to the NM-NAM as a URL in his browser. In fact, the embedded analysis software in the NM-NAM is for all intensive purposes exactly the same as the embedded analysis software in the NAM-1/2. The main differences are:

NAM-1/2:

- Switch Ports Reporting
- Switch Health Reporting
- VLAN Reporting
- MAC Hosts/Conversation Reporting
- MPLS Reporting
- Support for Switch Alarms

NM-NAM:

- Router Interface Reporting
- Router Health Reporting
- NBAR Reporting
- No VLAN, MPLS or MAC Reporting

After Dean enters the URL for the NM-NAM, he is presented with the Traffic Analyzer login screen. He logs into the NM-NAM using the account information that he defined during installation (see Chapter 4 for more details) and clicks the **Login** button. The Traffic Analyzer authenticates his login information and displays the System Resources metrics. Dean reviews the System Resources metrics to ensure that the NM-NAM has sufficient memory and CPU to accommodate his monitoring tasks because he knows that lack of memory or CPU could mean that the NM-NAM might inaccurately collect and report statistics. If resource utilization rises too high, he knows to reduce the number of monitoring tasks he has configured to relieve the performance burden on the NM-NAM.

Scenario 2

Setting Router Parameters

Setup > Router Parameters > Router Information

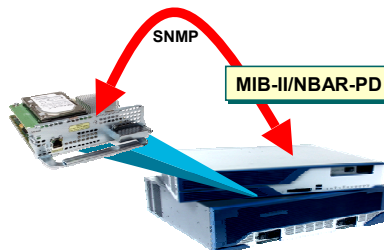
Router System Information	
Name:	nmtg-hq-core-3725
Hardware:	3725 chassis, Hw Revision: 1
Router Software Version:	Version 12.3(4)
Router System Uptime:	19 days, 21 hours
Location:	N/A
Contact:	N/A
Router IP Address:	192.168.159.21
SNMP Read-Write Community String:	XXXXXXXXXX
Verify String:	XXXXXXXXXX
<input type="button" value="Test"/> <input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Enter the same IP address (internal analysis int) and read-write community string as was configured on the router.

The NM-NAM needs to know the router's community strings in order to retrieve interface statistics.

Setup > Router Parameters > NBAR Protocol Discovery

NBAR Status
Current Status: Partially Enabled
NBAR is activated on a subset of interfaces, and the NAM can provide NBAR statistics for these interfaces. Other interfaces may not have the NBAR feature enabled. You can use the 'Details' button to view more detailed interface information, and if necessary, click the 'Enable' button to activate NBAR on all switches.
This can have an impact on the switch performance.
<input type="button" value="Details"/> <input type="button" value="Save"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/>



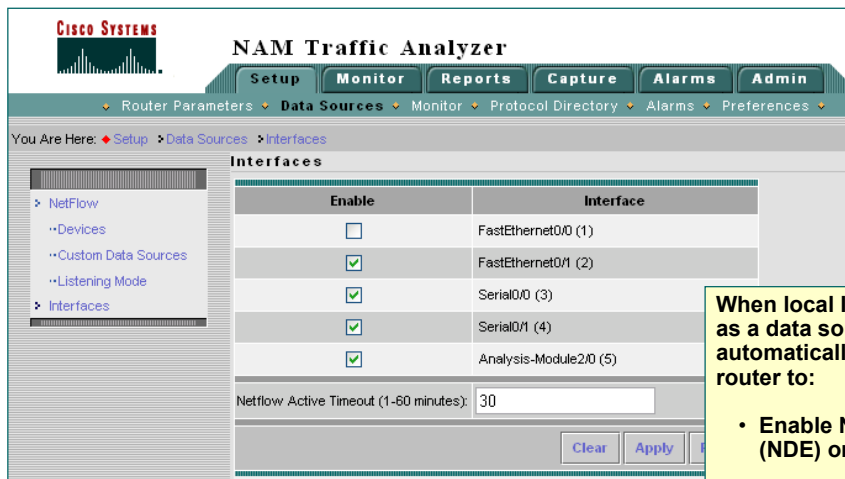
Setting Router Parameters

The first indication of potential troubles in a network are often detected by change in the utilization of an interface. Dean, therefore, wants to configure the NM-NAM to retrieve interface statistics from the host router via SNMP. To configure the NM-NAM with the router's SNMP community strings, Dean performs the following steps:

- Step 1. Click **Setup > Router Parameters > Router Information**. The Router System Information dialog box is displayed.
- Step 2. Enter the **IP Address** of the Router configured during NAM installation and the correct **read-write community strings** as configured on the host router and click **Apply** to store in the NAM memory.
- Step 3. Click the **Test** button to verify that the strings were entered correctly. Click **OK** to close the verify window.
- Step 4. Dean also checks to see that NBAR is enabled on the Router so he can retrieve the applications discovered on each interface. Click **Setup > Router Parameters > NBAR Protocol Discovery**. The NBAR Status dialog is displayed. Verify that NBAR is enabled. If not, select enable. (If using IOS then click Save for the changes to be written to the start-up config).
- Step 5. To see details of which interfaces are enabled for NBAR, click **Details**.

Scenario 2

Configuring Interfaces as Data Sources



When local Interfaces are enabled as a data source, the NM-NAM will automatically interact with the router to:

- Enable NetFlow Data Export (NDE) on the router Interfaces
- Set itself as the destination for NDE

Provides Application, Host, and Conversation data with no further set-up

Configuring Interfaces as Data Sources

By default the NM-NAM will query the MIB-II parameters on the host router to retrieve basic statistics for each interface (much like the mini-RMON stats on the NAM-1/2). Typically, viewing the interface utilization stats would help determine which traffic to forward to the NM-NAM for more depth analysis. To provide you with some deeper analysis prior to forwarding the traffic via CEF to the NM-NAM, the NM-NAM can configure the router to forward interface traffic via NetFlow to itself for application, hosts, and conversation statistical analysis. Dean uses the following steps to configure this feature:

- Step 1. Click **Setup > Data Sources > Interfaces**. The Interfaces dialog box is displayed showing a list of all interfaces on the host router.
- Step 2. Enable the desired interfaces in which to forward NetFlow traffic to the NM-NAM and click **Apply**.

The NM-NAM will now configure the host router to enable NetFlow on the selected interfaces and set itself as the destination.

Scenario 2

Interface Utilization

Monitor > Router > Interface Stats

<input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data													
Filter: <input type="text"/>												<input type="button" value="Filter"/>	<input type="button" value="Clear"/>
Showing 1-3 of 3 interfaces													
#	Interface	In % Utilization	Out % Utilization	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Non-Unicast/s	Out Non-Unicast/s	In Discards/s	Out Discards/s	In Errors/s	Out Errors/s
1.	Se0/0	0.00	0.00	1.81	2.02	339.54	43%	485.38	0.19	0.17	0.00	0.00	0.00
2.	Fa0/1	0.00	0.00	1.17	1.24	265.66	34%	220.08	0.17	0.18	0.00	0.00	0.00
3.	An2/0	0.00	0.01	1.25	3.81	187.24	24%	735.57	0.02	0.15	0.00	0.00	0.00

Rows per page: Units: Go to page: of 1

Select an item then take an action -->

Check interface usage for any indication of problems.

Select interface and click Details for application, host, and conversation statistics

See next page

Interface Utilization

Dean can now look at the utilization of each of the host Router's interfaces.

Step 1. Click **Monitor > Router > Interface Stats**. The Interface Stats report is displayed.

Most of the monitor views offer three perspectives—Current Rates, TopN Chart, and Cumulative Data. These can be chosen by clicking the radio buttons at the top of the data table. By default, the Current Rates table is displayed first when Port Stats is chosen. This table provides statistics for traffic collected during the last refresh cycle only. The TopN chart provides a list of ports ranked by volume for data during the last refresh cycle only, and the Cumulative Data table provides absolute values for data collected since the min-RMON counters were last cleared.

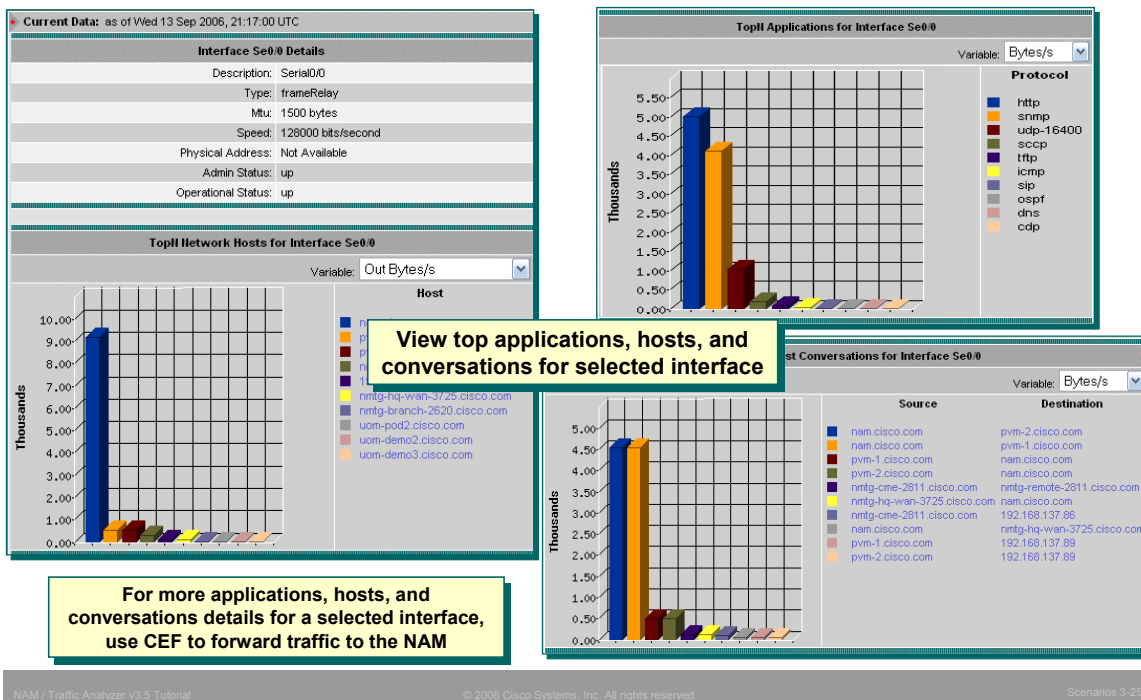
The refresh cycle can be modified by selecting Setup > Preferences, changing the Refresh Interval, and clicking Apply. If the Auto Refresh check box is selected on any data screen, the tables and charts will be refreshed as new data is collected.

Using these views, Dean happily notes that all connected interfaces on the core branch router are barely utilized. This confirms the bandwidth predictions Q-Bits used to design its network. If any abnormally high utilization or error conditions had existed, Dean could use them to help determine where to begin looking for the causes.

Since the serial link is connected to the WAN, Dean decides to probe it a little. He selects Se0/0 and clicks **Details**.

Scenario 2

Interface Details



Interface Details

Dean is now presented with application, host, and conversation statistics for the selected interface. This is the NetFlow data forwarded from the interfaces setup using Setup > Data Source > Interfaces.

The graphs presented are similar to the graphs displayed when selecting Monitor > Overview. They provide Dean with a good high-level view of the traffic and its users for the selected interface.

Scenario 2

Interface NBAR

You Are Here: [Monitor](#) > [Router](#) > [NBAR](#)

Monitor > Router > NBAR

Supervisor Protocol Discovery

Per-Second Data: as of Mon 16 Oct 2006, 18:29:23 UTC

☒ Auto Refresh

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Interface: **Fa0/0** Protocol:

Showing 1-8 of 8 records

#	Protocol's	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Bit Rate/s	Out Bit Rate/s
1.	skinny	2.10	86%	0.11	183.38	6.98	0.00
2.	http	0.20	8%	0.18	12.39	84.25	0.00
3.	icmp	0.03	1%	0.03	2.56	2.56	0.00
4.	dhcp	0.03	1%	0.02	12.03	6.00	0.00
5.	dns	0.03	1%	0.03	2.66	5.41	0.00
6.	sip	0.03	1%	0.07	20.95	26.70	0.00
7.	ospf	0.00	<1%	0.10	0.00	8.85	0.00
8.	unknown	0.00	<1%	0.07	0.00	4.20	0.00

Rows per page: **15** Units: **Bytes/s** Go to page: **1** of 1

Use NBAR to find out application details per interface for any indication of problems.

Interface NBAR

Before configuring the NM-NAM for more in-depth monitoring of the WAN link, Dean decides to also view what applications NBAR has discovered on the WAN link.

- Step 1. Click **Monitor > Router > NBAR**. The NBAR report is displayed.
- Step 2. Select **Se0/0** (the WAN link) from the pull down source menu. Notice that all interfaces are listed in the pull down menu regardless if they are operational or not. Selecting a non-operational interface will simply provide no data and a Warning message as to the probable reason for no data.

Dean notes that currently approximately 6% of the traffic seen is unknown (other). This is more than likely the proprietary traffic that Dean wants to classify to get an idea of how much of the WAN links bandwidth it is utilizing.

To do this, Dean needs to configure the Router to send all traffic on the WAN link to the NAM for analysis.

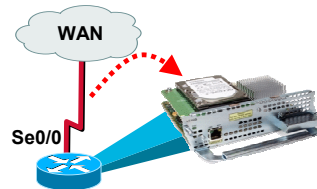
Scenario 2

Configure Data Source and Monitoring

Step 1: Select NAM Data Source

```
Telnet <NAM Host Router IP Address>
Router > configure terminal
Router (config)# ip cef
Router (config)# interface Se0/0
Router (config-if)# analysis-module monitoring
```

1. Enable Cisco Express Forwarding.
2. Select interface.
3. Forward packets to NAM.



Step 2: Configure Core Monitoring (Setup > Monitor > Core Monitoring)

Data Source: Internal	
Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	100
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	500
Check desired functions then Apply -->	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Enable Application, Host, and Conversation monitoring for the Internal NM-NAM interface

NM-NAM Data Source and Collection Configuration

To analyze all traffic on the WAN link, Dean uses the following steps:

- Step 1. From a Command window on his desktop machine, Dean telnets to the router that hosts the NM-NAM and enters configuration mode.
- Step 2. First, he enables Cisco Express Forwarding on the router by entering the command **ip cef**.
- Step 3. Next he enters the interface configuration mode for the WAN link using the command **int Se0/0**.
- Step 4. Next he configures the router to forward a copy of all packets coming to or from Se0/0 to the NAM with the command **analysis-module monitoring**. He could forward packets from other interfaces in the same way. When configuration is complete he exits the router.
- Step 5. Next Dean must enable monitoring for the traffic being sent by CEF to the internal interface of the NAM. Click **Setup > Monitor > Core Monitoring**. The Core Monitoring Functions dialog is displayed.
- Step 6. The pull-down Data Sources list displays the two interfaces for the NM-NAM and any configured NDE data sources. Select **Internal** from this menu to enable monitoring.
- Step 7. Enable desired monitoring functions (application, network host, network conversations) and click **Apply**.

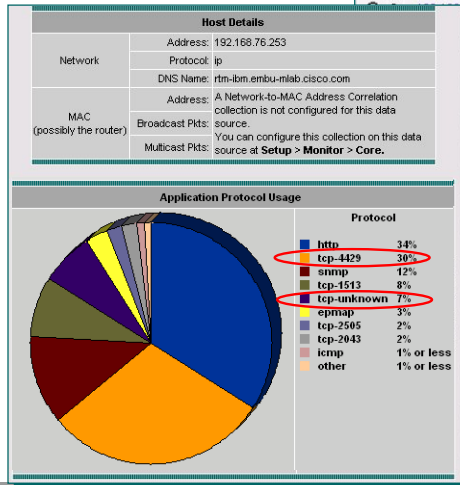
All packets to/from Se0/0 are now being copied to the Internal NM-NAM interface and are being analyzed.

Scenario 2

Top Hosts

Monitor > Hosts > Network Hosts

Select Host for Capture



Current Rates TopN Chart Cumulative Data

Data Source: Internal Address: Filter Clear

Showing 1-5 of 99 records

#	Address	Via	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	Non-Unicast/s
1	lzo-dan-lan-vlan1-dhcp16.cisco.com	ip	2041.00	2087.00	1471769.00	255755.00	0.00
2	rtm-ibm.embu-mlab.cisco.com	ip	1779.88	1300.62	192199.54	877920.40	0.01
3	128.100	ip	1299.64	1778.96	877610.42	190922.85	0.00
4	embu-mlab.cisco.com	ip	769.00	770.00	96385.00	95849.00	0.00
5	embu-mlab.cisco.com	ip	18.32	18.59	2109.86	2200.84	0.18

Go to page: 1 of 20

Details Capture Real-Time Report

Host Drill Down

- Use data capture to determine what is the "tcp-unknown" traffic
- Traffic Analyzer can automatically discover up to 100 unknown protocols. The protocols are displayed according to the parent protocol and port (i.e. tcp-4429).

Top Hosts

Knowing some of the clients and servers responsible for the proprietary application, Dean decides to view a Host report to see what their behavior is, and the launch a Quick Capture to help him find and classify the proprietary traffic.

- Step 1. Click **Monitor > Hosts > Network Hosts**. The Network Hosts report is displayed. Make sure that the Data Source for the displayed information is the Internal NM-NAM interface by selecting Internal from the Data Sources pull down list.
- Step 2. Dean locates one of the servers and click on its name to drill down into its behavior. The Hosts Drill Down report displays all protocols in use by this hosts and the conversations for each protocol. Dean notes that some traffic by this host is classified as "tcp-unknown" traffic or in all likelihood the proprietary traffic he wishes to classify.
- Step 3. Returning to the Network Hosts report, Dean selects the host, and clicks **Capture** to begin capturing packets to and from this host.

Note: The capture begins immediately if buffer space is available and the decode screen is displayed.

Scenario 2

Quick Capture Settings Review

Capture > Buffers

The screenshot shows the 'Capture Buffers' window with a table of buffers and a 'Settings' button. A red arrow points from the 'Settings' button to the 'Buffer Settings' dialog. The dialog shows the 'Capture Name' as 'HOST_192_168_76_253' and the 'Capture Status' as 'Running'. The 'Capture Filter' is set to 'IP' with 'Source' as '192.168.76.253' and 'Both Directions' checked. The 'Buffer Size' is '10 MB' and 'Packet Slice Size' is '500 Bytes'. The 'Buffer Full Action' is 'Lock'. The 'Settings automatically filled in by Quick Capture' label points to the 'Source' field.

Name	Owner	Start Time	Buffer Size	Packets	Status
HOST_192_168_76_253	LocalMgr	Wed 15 Jun 2005, 18:00:25	10 MB	6302	Running
Automatic_Capture	NAM Alarm (not set)	-	0 MB	0	Cleared (Disabled)

Available buffer space: 59.3 MB available

Automatically created buffer: HOST_192_168_76_253

Buffer Status: Running

Buffer Parameters: 10 MB, 500 Bytes

Filter by Address: 192.168.76.253

Buffer Controls: Start, Pause, Clear, Decode, Close

Reviewing the Data Capture Setup

Before looking at the decode of the captured packets that is immediately displayed, let's take a quick look at the buffer that was automatically setup. The buffer parameters dialog is also used for controlling the capture. To review the automatically created buffer:

- Step 1. Click **Capture > Buffers**. The list of Buffers is displayed.
- Step 2. Locate the desired buffer (name of buffer in this case will be Host_IP_Address). Click **Settings**. The Capture Settings dialog is displayed.

Note: The filter settings were automatically set to collect all packets to/from this host.

Dean now looks at the decoded packets to try and figure out what the tcp-unknown traffic is.

Scenario 2

Decoding the Packets

CISCO SYSTEMS NAM Traffic Analyzer - Packet Decoder
HOST_192_168_76_253

Packets: 1-1000 of 1233 [Stop] [Prev] [Next] 1000 [Go to] 1 [Display Filter] [TCP Stream]

Pkt	Time(s)	Size	Source	Destination	Protocol	Info
15	0.000	162	rtm-ibm.embu-mlab.ci...	192.168.78.100	TCP	666 > 3256 [PSH, ACK] Seq=4287402867 Ack=25...
16	0.000	68	rtm-ibm.embu-mlab.ci...	192.168.78.100	TCP	666 > 3256 [FIN, ACK] Seq=4287402967 Ack=25...
17	0.001	362	192.168.78.100	rtm-ibm.embu-mlab.ci...	TCP	3257 > 2020 [PSH, ACK] Seq=2517932045 Ack=4...
18	0.001	1062	rtm-ibm.embu-mlab.ci...	192.168.78.100	TCP	2020 > 3257 [PSH, ACK] Seq=4287453773 Ack=2...
19	0.001	68	rtm-ibm.embu-mlab.ci...	192.168.78.100	TCP	2020 > 3257 [FIN, ACK] Seq=4287454773 Ack=2...
20	0.001	68	192.168.78.100	rtm-ibm.embu-mlab.ci...	TCP	3255 > 2020 [ACK] Seq=2517852877 Ack=42873...
21	0.001	1522	rtm-ibm.embu-mlab.ci...	192.168.78.100	TCP	2020 > 3255 [ACK] Seq=4287363350 Ack=25178...
22	0.001	1522	rtm-ibm.embu-mlab.ci...	192.168.78.100	TCP	2020 > 3255 [ACK] Seq=4287364810 Ack=25178...

Packet Number: 18 - Time: Jul 27, 2005 18:26:20.153 - Packet Length: 1062 bytes - Capture Length: 1062 bytes

- + **ETH** Ethernet II, Src: 00:02:55:54:74:eb, Dst: 00:00:0c:07:ac:01
- + **VLAN** 802.1q Virtual LAN
- + **IP** Internet Protocol, Src Addr: rtm-ibm.embu-mlab.cisco.com (192.168.76.253), Dst Addr: 192.168.78.100 (192.168.78.100)
- **TCP** Transmission Control Protocol, Src Port: 2020 (2020), Dst Port: 3257 (3257), Seq: 4287453773, Ack: 2517932345, Len: 1000
- TCP** Source port: 2020 (2020)
- TCP** Destination port: 3257 (3257)
- TCP** Sequence number: 4287453773
- TCP** Next sequence number: 4287454773

0000 00 00 0c 07 ac 01 00 02 55 54 74 eb 81 00 00 64UTt...
0010 08 00 45 00 04 10 f9 d8 40 00 80 06 e0 5c c0 a8 ..E.....\..
0020 4c fd c0 a8 4e 64 07 e4 0c b9 ff 8d 5a 4d 96 14 L...Nd.....ZM..
0030 99 39 50 18 43 44 ea 70 00 00 74 20 61 20 66 69 .9P.CD.p..t a fi
0040 6c 65 20 61 73 20 61 20 64 61 74 61 62 61 73 65 le as a database
0050 20 6f 66 20 64 65 66 69 6e 69 74 69 6f 6e 73 20 of definitions
0060 6f 66 0a 3e 66 75 6e 63 74 69 6f 6e 73 2c 20 64 of.>functions, d
0070 61 74 61 2c 20 73 74 72 75 63 74 75 72 65 73 2c ata, structures, d
0080 20 6f 66 20 64 65 66 69 6e 69 74 69 6f 6e 73 2c ..t..sh..

Decoding the Packets

If the Decode window that was automatically opened when the Quick Capture was selected was closed, Dean could always view the decode by selecting **Decode** from the **Capture > Buffers** dialog with the buffer to decode selected.

The Packet Decoder screen provides details of the captured packets. The top window provides a summary of the packet, including size, source and destination, the highest-layer protocol decoded, and other information based on the decoded protocol type. Dean can see that the “other” traffic is TCP traffic because that is the highest layer decoded—no application information is available. Selecting a packet and looking at the lower window gives a layered breakdown of the details. Dean can see that TCP ports 2020 are used. Looking at the raw data for one of the packets, Dean notices that this is a Q-Bits database GUI tool in development. Dean will next add it to the Protocol directory to monitor it by name.

Scenario 2

Adding a New Protocol

Setup > Protocol Directory > Individual Applications

The screenshot shows the 'Protocol Directory' table and the 'New Protocol Parameters' dialog box. The table lists various protocols, and the dialog box shows the configuration for a new protocol. Annotations highlight key steps: selecting TCP as encapsulation, entering the port number and name, and clicking the 'Create' button.

#	Protocol	Identifier	Port Range	Addr Map Stats	Host Stats	Conv Stats	ART Stats
1.	aarp	33011	1	n/a	n/a	n/a	n/a
2.	acap	674	1	n/a	✓	✓	✓
3.	acap	674	1	n/a	✓	✓	✓
4.	acap	674	1	n/a	✓	✓	✓
5.	acap	674	1	n/a	✓	✓	✓
6.	adsp	7	1	n/a	✓	✓	n/a
7.	aep	4	1	n/a	✓	✓	n/a
8.	afp	1	1	n/a	✓	✓	n/a
9.	agentx	705	1	n/a	✓	✓	✓
10.	agentx	705	1	n/a	✓	✓	✓

Rows per page: 10 Go to page: 1 of 164

Annotations:

- Select Encapsulation:** Points to the 'TCP' option in the 'New Protocol is encapsulated within' list.
- Enter port number and name:** Points to the 'TCP port (0..65535): 2020' and 'Name: w-ether2.ip.tcp.QbitsDB' fields.
- Enter number of continuous ports used by application:** Points to the 'Port Range (1-255): 1' field.
- Create:** Points to the 'Create' button in the 'Protocol Directory' table.

Adding a New Protocol

Because this is a legitimate application, Dean will add it as a new protocol to be monitored in order to reduce the size of the “other” traffic. To add a new protocol for monitoring, Dean performs the following steps:

- Step 1. Select **Setup > Protocol Directory > Individual Applications**. The Protocol Directory screen is displayed listing all currently defined protocols the NAM knows about.
- Step 2. Select **Create**. The first dialog of the Create New Protocol wizard is displayed.
- Step 3. Select the protocol that the new protocol is encapsulated within—TCP in this case. Select **Next>**. The second dialog of the Create New Protocol wizard is displayed.
- Step 4. Enter the TCP port that this new protocol uses—**2020**. Enter the application name—**QbitsDB**. **Note:** Add the name after the encapsulation string. **Note:** If the application uses a number of consecutive ports, this one definition can cover them all by entering the number of ports used (Ports Range) starting from the one enter above. Click **Submit**.

The NAM will now categorize this traffic in the QbitsDB bucket instead of the “other” bucket. This gives Dean more immediate insight into how applications are using network resources.

Scenario 2

New Application View

Monitor > Apps > Individual Applications

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source:

Showing 1-10 of 41 records

#	Protocol	Packets/s	Bytes/s	
1.	http	9.07	3,938.41	23%
2.	snmp	16.54	3,896.52	23%
3.	QbitsDB	4.40	2,727.13	16%
4.	hsrp	22.54	1,577.88	9%
5.	ftp-data	9.74	1,568.01	9%
6.	sccp	3.19	997.14	6%
7.	ospf	7.65	759.08	4%
8.	arp	7.33	498.69	3%
9.	tcp-unknown	3.45	353.04	2%
10.	telnet	0.17	116.90	1%

Rows per page: Units: Go to page: of 5

Previously "tcp-unknown" traffic is now reclassified providing a more detailed picture of applications on the network

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-32

New Application View

Dean now looks at the Application report to see that the proprietary application has been reclassified in the reports.

Step 1. Select **Monitor > Apps > Individual Applications**. Ensure **Internal** is the selected Data Source. The Applications report is displayed

Dean can now easily see the impact the QbitsDB application has to the WAN link. Dean also notices that the "tcp-unknown" traffic has been reduced.

CISCO SYSTEMS



Performance/Troubleshooting (NAM-1/2)

Performance/Troubleshooting (NM-NAM)

QoS Monitoring

VoIP Monitoring

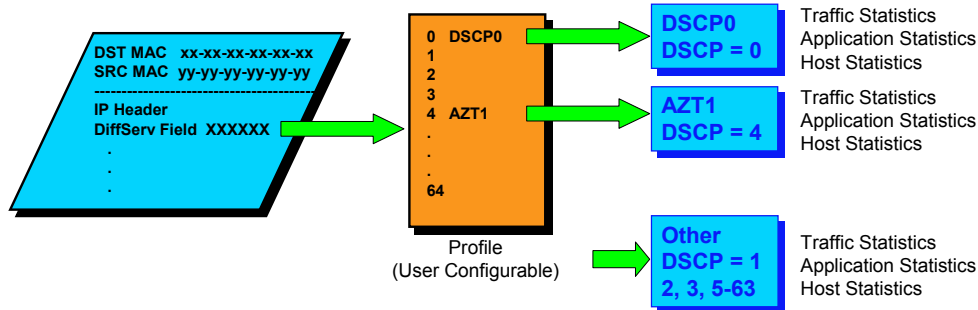
Trend Analysis



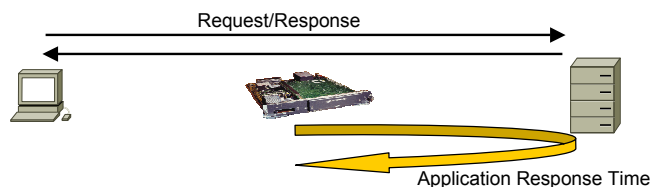
Scenario 3

QoS Monitoring (Using DiffServ and ART)

Differentiated Services Monitoring



Application Response Time



Scenario 3 - QoS Monitoring (Using DiffServ and ART)

Networks today increasingly incorporate quality-of-service (QoS) technologies to prioritize traffic. The NAM provides several monitoring features to allow you to view prioritized traffic to help ensure proper configuration and to minimize misuse.

The Differentiated Services field in the IP header portion of a packet can be set to a value between 0 and 63 (Differentiated Services Code Point [DSCP] value). The network infrastructure equipment can then process the packets for forwarding according to this value. The use of DSCP values, and the configuration of the networking equipment to utilize them in forwarding decisions, allows the network designer to implement different levels of services for different applications based on the DSCP value.

The NAM can collect statistics based on the DSCP value in much the same way as it collects statistics per VLAN. This gives the network manager the ability to verify and monitor a QoS implementation. The NAM can also measure application response times for a server to ensure that service levels are being met.

Dean wants to see what server farm (port Gi1/2) traffic is currently using DSCP values and check to see if any of the servers are experiencing slow response times. If so, Dean knows that he can reconfigure some of the network infrastructure equipment to give a higher priority to the server traffic. To perform this scenario, Dean needs to create a Differentiated Services (DiffServ) profile, enable monitoring for the profile, view results, enable the Application Response Time (ART) feature for desired traffic, and view those results.

Scenario 3

Create DiffServ Profile

Setup > Monitor > DiffServ > Profile

Create a generic profile to determine what DSCP values are currently set.

Select Template and Edit field names if desired (named fields create collection buckets).

DSCP Value	Group Description
0	DSCP0
1	DSCP1
2	DSCP2
3	DSCP3
4	DSCP4
5	DSCP5
6	DSCP6
7	DSCP7
8	DSCP8
9	DSCP9
10	DSCP10
11	DSCP11

Submit Reset

Create DiffServ Profile

The first step in monitoring traffic based on DSCP value is to create a profile that defines which DSCP values to collect for. Any values that are not explicitly configured are grouped into a catch-all statistics bucket call "Other DSCP." Dean will create a default template that creates a statistic bucket for every possible DSCP value. This way he can see exactly what values are currently being used on his network. After this exercise, he could create a new profile for just the values being used with descriptive names for the aggregation groups.

- Step 1. Select **Setup > Monitor > DiffServ Profile**. The DiffServ Monitor Profile screen lists existing profiles already defined.
- Step 2. Click **Create** to make a new profile. The DiffServ Profile Setup screen is displayed.
- Step 3. Numerous templates exist to help get you started, but using templates is optional. Entering a label for a DSCP value will create the statistics bucket with that name (More than one DSCP value can have the same label, this creates an aggregation group). For Dean's use, however, he selects a template from the Template pull-down list called No Aggregation that contains a label for every DSCP value.
- Step 4. He gives his template the name **QoSsearch** and clicks **Submit** to create it for use.

Scenario 3

Enable DiffServ Monitoring

Setup > Monitor > DiffServ > Monitoring

Data Source:	VLAN 100	Enable DiffServ statistics for the created profile on VLAN 100 (main VLAN for server farm).
DiffServ Profile:	QoSsearch	
	Monitoring Function	Max Entries
Enable Collection Statistics	<input checked="" type="checkbox"/> Traffic Statistics	Not applicable
	<input checked="" type="checkbox"/> Application Statistics	100
	<input checked="" type="checkbox"/> IP Host Statistics	100
Select an item then take an action -->		Apply Reset

Enable DiffServ Monitoring

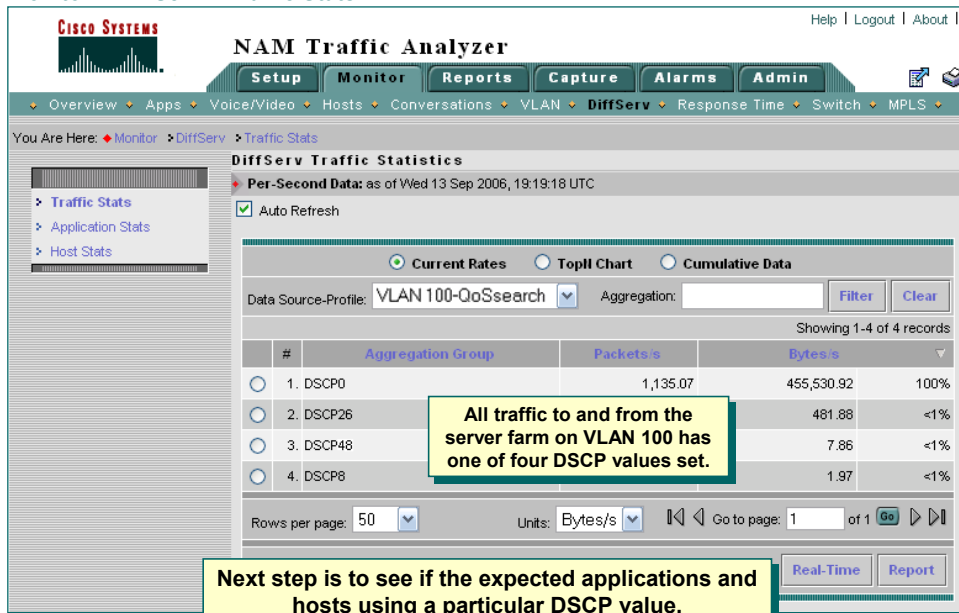
Like other types of collections on the NAM, no DiffServ data is actually collected until the monitoring is enabled on a data source. To enable DiffServ monitoring, Dean performs the following steps on the Catalyst 6500 Series NAM (NM-NAM follows the same steps):

- Step 1. Select the **Monitoring** option under the DiffServ heading from the menu on the left side of the screen (you should already be at **Setup > Monitor**). The DiffServ Monitor Setup screen is displayed.
 - Step 2. From the Data Source pull-down menu, Dean selects **VLAN 100**. (VLAN 100 is the main VLAN for the server farm. Remember, the span source is still port Gi1/2, which connects the distribution switch to the server farm workgroup access switch.)
 - Step 3. From the DiffServ Profile pull-down list, select **QoSsearch** (the profile just created).
 - Step 4. Enable all types of statistics collections. **Note:** You can change the number of applications and hosts the NAM collects statistics for by selecting 100, 500, or Max Possible from the associated Max Entries pull-down list.
 - Step 5. Click **Apply** to enable the collection of traffic, application, and host statistics based on the DSCP values for all packets on port Gi1/2, VLAN 100.
- Dean is now ready to look at the traffic based on DSCP values.

Scenario 3

DiffServ Traffic Statistics (VLAN 100)

Monitor > DiffServ > Traffic Stats



DiffServ Traffic Statistics

To view the traffic statistics for port Gi1/2, VLAN 100, based on DSCP values, Dean does the following:

- Step 1. Select **Monitor > DiffServ > Traffic Stats**. The DiffServ Traffic Statistics screen is displayed.
- Step 2. From the Data Source-Profile pull-down list, select **VLAN 100 QoSsearch** (enabled earlier for monitoring). The DiffServ Traffic Statistics screen for VLAN 100 QoS search is displayed.

Dean can instantly see that all traffic for VLAN 100 on this link is using one of three DSCP values as expected. Notice that there is no "other DSCP" group because all DSCP values have a label and are accounted for. Next, Dean will view which applications have traffic for the different DSCP values. (0 is the default so that probably would not be interesting to look at.)

Scenario 3

DiffServ Application Statistics (VLAN 100)

Monitor > DiffServ > Application Stats

Current Rates TopN Chart Cumulative Data

Data Source-Profile: VLAN 100-QoSsearch Protocol: Filter Clear

Aggregation: DSCP26

Showing 1-5 of 5 records

#	Protocol Name	Packets/s	Bytes/s
1. h225		0.35	30.45
2. sccp		0.42	30.13
3. tcp-2428		0.43	29.67
4. h245		0.37	28.62
5. mgcp		0.25	17.00

Go to page: 1 of 1 Go

Details Real-Time Report

Verify that the listed protocols are the only ones you configured to use the selected DSCP value.

Verify that only the expected servers are using a protocol with this DSCP value

Application Conversations - mgcp Group - DSCP26

Source	Destination	Packets	Bytes
embu-callingr1.embu-mlab.cisco.com	10.1.6.101	46	3128
embu-callingr1.embu-mlab.cisco.com	10.1.6.103	46	3128
embu-callingr1.embu-mlab.cisco.com	10.1.6.109	46	3128
embu-callingr1.embu-mlab.cisco.com	192.168.79.42	30	2040

Close

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-38

DiffServ Application Statistics

Dean wants to verify that only voice related protocols that he configured for DSCP value 26 are actually the only protocols transmitting with that value. To look at which applications are sending packets using certain DSCP values, Dean does the following:

- Step 1. Select **Monitor > DiffServ > Application Stats**. The DiffServ Application Statistics screen is displayed.
- Step 2. Select **VLAN 100-QoSsearch** from the Data Source-Profile pull-down list.
- Step 3. Select the DSCP value from the Aggregation pull-down list (DSCP 26). **Note:** This list will contain all possible aggregations (DSCP values with labels in the profile), not just the ones with traffic.

Dean is happy to see that the only protocols listed are the ones he expected. Had there been unexpected protocols listed, Dean could quickly resolve the aberration to Q-Bits QoS plan.

Dean next selects a protocol to view which hosts are transmitting using this protocol with a DSCP value set to 26. Besides clicking the protocol itself, Dean could also get the same results by selecting the radio button next to the protocol and clicking the **Details** button. As expected, Dean only sees the Call Manager server using the various voice protocols.

Scenario 3

DiffServ Host Statistics (VLAN 100)

Monitor > DiffServ > Host Stats

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source-Profile: **VLAN 100-QoSsearch** Address:

Aggregation: **DSCP26**

Showing 1-5 of 8 records

#	Address	Type	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s
1	wan-3600a.embu-mlab.cisco.com	ip	0.45	0.00	36.58	0.00
2	10.1.6.103	ip	0.23	0.00	16.07	0.00
3	10.1.6.101	ip	0.17	0.00	11.33	0.00
4	10.1.6.109	ip	0.17	0.00	11.33	0.00
5	192.168.79.42	ip	0.12	0.00	7.93	0.00

Rows per page: **5** Go to page: **1** of 2

Verify that traffic from these hosts are eligible to send/receive application traffic using DSCP 26.

Verify that the listed hosts are using expected protocols and conversing with expected servers.

Host Conversations - wan-3600a.embu-mlab.cisco.com Group - DSCP26

Source	Application	Destination	Packets	Bytes
embu-callingr1.embu-mlab.cisco.com	h245	wan-3600a.embu-mlab.cisco.com	379	28556
embu-callingr1.embu-mlab.cisco.com	h225	wan-3600a.embu-mlab.cisco.com	402	34853

DiffServ Host Statistics

An alternate method to viewing DiffServ would be to look at all hosts transmitting for a given DSCP value. To look at which hosts are sending packets with certain DSCP values set, Dean does the following:

- Step 1. Select **Monitor > DiffServ > Host Stats**. The DiffServ Application Statistics screen is displayed.
- Step 2. Select **VLAN 100-QoSsearch** from the Data Source-Profile pull-down list.
- Step 3. Select the DSCP value you wish to view from the Aggregation pull-down list (DSCP-26). Notice that this list contains all possible aggregations (DSCP values with labels in the profile), not just the ones with traffic.

To further validate these hosts for DSCP-26, Dean clicks on the hosts to view which protocol they are using and with which server they are communicating. Again as expected, all conversations using DSCP-26 are with the Call Manager and use a voice related protocol.

Because Dean knows that voice-over-IP (VoIP) traffic is very sensitive to variations in network performance, he decides to monitor the Cisco CallManagers for response times to see how well the new network and the DiffServ implementation is supporting voice traffic. Slow response times could indicate improperly configured QoS mechanisms or a slow server.

Note: To collect ART statistics, the Switched Port Analyzer (SPAN) source must include both directions in order to see both the request and response packets.

Scenario 3

Enable ART Monitoring (VLAN 100)

Setup > Monitor > Response Time Monitoring

DataSource	
<input type="checkbox"/>	ALL SPAN
Select a control row then take an action --	
Create	Edit Delete

Select data source to enable ART on and configure the report interval and response buckets

Response Time Collection Configuration	
DataSource	VLAN 100
Report Interval (30 - 604800 sec)	1800
RspTime1 (msec)	5
RspTime2 (msec)	15
RspTime3 (msec)	50
RspTime4 (msec)	100
RspTime5 (msec)	200
RspTime6 (msec)	500
RspTimeMax (msec)	3000
Max Entries in Tables	500
Submit Reset	

Instructions:
Use this window to specify settings for response time monitoring. When you specify settings for response time buckets (RspTime1 to RspTimeMax), make sure each subsequent setting is larger than the previous (RspTime1 <= RspTime2 <= RspTime3 <= RspTime4 <= RspTime5 <= RspTime6 <= RspTimeMax).

Collection starts when you click **Submit**. Results are available after the first interval.

Enable ART Monitoring (VLAN 100)

Again, like any other monitoring activity on the NAM, Application Response Time (ART) monitoring must first be enabled before any statistics can be collected. You may recall from our discussions in Chapter 2 that ART results can have very different values based on the NAM location. The closer you place the NAM to the server you want to monitor, the more your response time values will reflect server think time. The closer you position the NAM to the client, the more your response time values will reflect transaction time.

To enable ART monitoring, Dean does the following:

- Step 1. Select **Setup > Monitor > Response Time Monitoring**. The Response Time Monitoring Setup screen is displayed, listing any currently active ART monitoring.
- Step 2. ART is enabled on a per-VLAN basis. If the VLAN you wish to enable ART for is not displayed, select **Create**; otherwise, select the VLAN and click **Edit**. The Response Time Monitoring Setup, Collection Configuration screen is displayed.
- Step 3. Select the VLAN, **VLAN 100**, you wish to enable ART for from the Data Sources pull-down list.
- Step 4. ART values by default are reported every 30 minutes. The time for each response pair is attributed to one of six buckets. Also the number of pairs, maximum and minimum time, and average are reported for each client/server pair seen on the monitored data source. You can change any of the listed values; click **Submit** to enable the ART monitoring for the selected data source.

Scenario 3

ART Server Data (VLAN 100)

Cisco Systems NAM Traffic Analyzer

Help | Logout | About |

Setup Monitor Reports Capture Alarms Admin

Overview Apps Voice/Video Hosts Conversations VLAN DiffServ Response Time Switch MPLS

You Are Here: Monitor > Response Time > Server

Server Response Time

Latest Data: 180 second interval ending Wed 13 Sep 2006, 19:43:45 UTC

☒ Auto Refresh

Data Source: VLAN 100 Server Filter Clear

Showing 1-5 of 67 records

#	Server	Protocol	Clients	Avg Resp Time	Min Resp Time	Max Resp Time	Retries	Late Responses
1.	cilantro.embu-mlab.cisco.com	telnet	31	19	0	195	0	0
2.	cilantro.embu-mlab.cisco.com	ntp-session	9	1	0	195	0	0
3.	cilantro.embu-mlab.cisco.com	smb	9	11	0	3233	0	2
4.	embu-callmgr1.embu-mlab.cisco.com	sccp	7	2	0	171	0	0
5.	embu-callmgr2.embu-mlab.cisco.com	sccp	7	150	102	205	0	0

Rows per page: 5 Go to page: 1 of 14

Select an item then take an action -->

Details Capture Report

Zoom in for more details

ART Server Data

Dean is ready to view how the Cisco CallManager application is performing. Based on the placement of the NAM in the distribution switch, the times reported will be from the distribution switch, to the server farm workgroup access switch, to the Cisco CallManager, and back. It would be better to have the NAM in the server farm workgroup access switch in order to get server think time, but Dean will have to wait until he upgrades that switch to a Cisco Catalyst® 6500 Series. Remember that no data will be available for at least 30 minutes. To see the server response times, Dean does the following:

Step 1. Select **Monitor > Response Time > Server**. The Server Response Time screen is displayed.

Step 2. Select **VLAN 100** from the Data Source pull-down list.

Dean sees the two Cisco CallManager application hosts listed and their response-time statistics. Using this data, Dean can see that one of the Cisco CallManagers is responding better than the other. This could be due to many factors, including configuration, but at least now Dean has data to use as a starting point. It is important to note that the data displayed is for the last ART interval which, by default, is 30 minutes; however, if a more granular resolution is needed, the interval can be lowered down to 30 seconds.

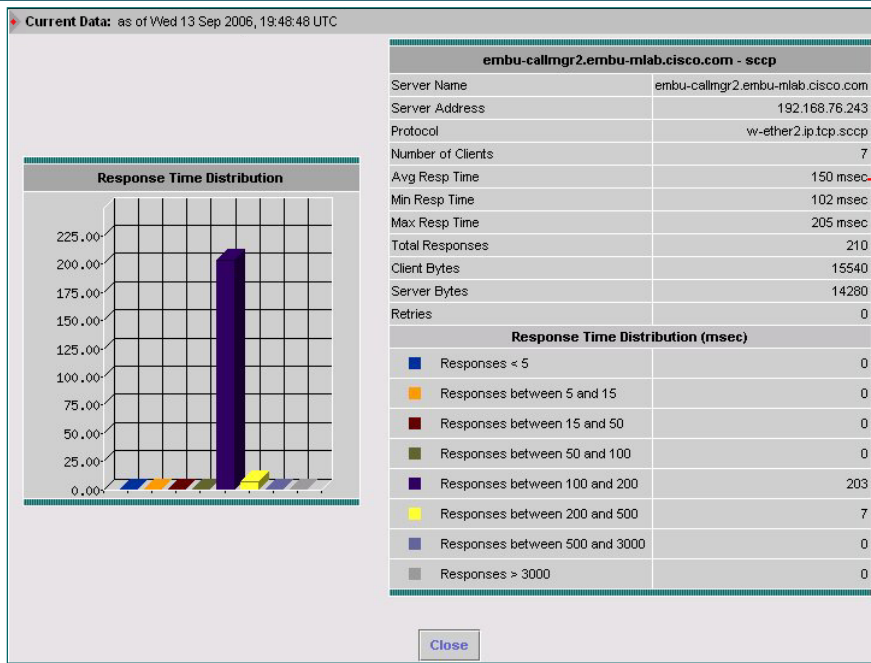
To see more details about the response time statistics for any listed server:

Step 3. Select the server you wish to view more details about.

Step 4. Click **Details**.

Scenario 3

ART Server Detail Data (VLAN 100)



**Too Slow?
Need more
information...
single client
slow or all?**

ART Server Detail Data

The ART Server Details report opens in a new window. Dean uses this report to see the number of responses and their time grouping. Almost all the response pairs fell into the same time bucket, indicating that the voice application is very consistent. Many times this will not be the case and Dean will want to drill down further to see if one particular client is experiencing slow application response time or if all clients are. Again, the more data Dean has, the easier it will be to isolate and correct any problems.

Scenario 3

ART Client Server Data (VLAN 100)

Monitor > Response Time > Client/Server

Showing 1-5 of 10 records

#	Server	Client	Protocol	Avg Resp Time	Min Resp Time	Max Resp Time	Retries	Late Responses
1	embu-callmgr2.embu-mlab.cisco.com	chariot-3500-1.embu-mlab.cisco.com	sccp	165	113	202	0	0
2	embu-callmgr2.embu-mlab.cisco.com	10.1.4.102	sccp	159	105	203	0	0
3	embu-callmgr2.embu-mlab.cisco.com	demo-2948.embu-mlab.cisco.com	sccp	155	104	202	0	0
4	embu-callmgr2.embu-mlab.cisco.com	192.168.79.36	sccp	155	107	201	0	0
5	embu-callmgr2.embu-mlab.cisco.com	192.168.76.26	sccp	154	102	204	0	0

Rows per page: 5

Go to page: 1 of 2

Details Capture Report

Zoom In for More Details

Response times are consistent for all clients

You can view response time by client server pairs to see if any QoS or other modifications need to be made.

ART Client Server Data

Dean decides he wants to review response-time statistics for traffic between an IP phone and the Cisco CallManager. To do so, he does the following:

- Step 1. Select **Monitor > Response Time > Client/Server**.
- Step 2. Select **VLAN 100** from the Data Source pull-down list.
- Step 3. Use the Filter option to select clients of server embu-callmgr2. The Client/Server Response Time report is displayed. This report displays the summary response-time statistics for each client/server pair seen during the last response-time interval.

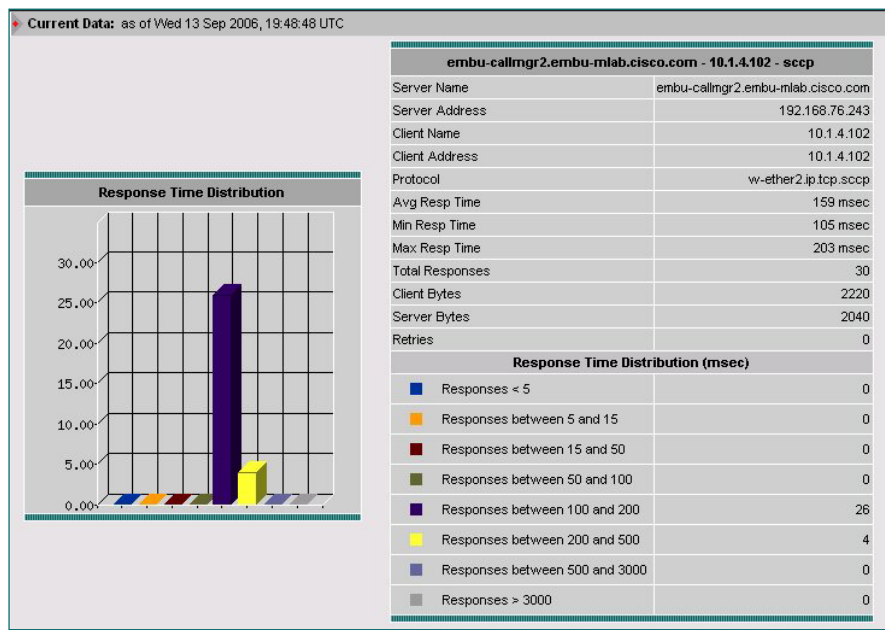
Dean notes that all clients using the embu-callmgr2 host are experiencing similar response times, but the clients attaching to the other Cisco Call Manager are experiencing much quicker response times. The difference in performance between these two Cisco Call Managers may be due to many things, including configuration or the load on the server, but it can also be due to the proximity of the NAM to the server and clients. Again, Dean now has facts to help isolate problems.

To see the time bucket breakdown for any client/server pair:

- Step 4. Highlight the client/server pair to see more information about, and click **Details**. (see next page)

Scenario 3

ART Client/Server Detail Data (VLAN 100)



ART Client/Server Detail Data

The ART Client/Server Details report opens in a new window. Dean uses this report to see the number of responses and their time grouping. In this case, some of the response pairs fall into the 200-500 ms time bucket, indicating that response time is a little high for this Cisco Call Manager / IP phone pair.

Again, the more data Dean has, the easier it will be to isolate and correct any problems. Dean will use some of the voice monitoring features of the Traffic Analyzer in the next scenario to gather more information about voice services on his network.

CISCO SYSTEMS



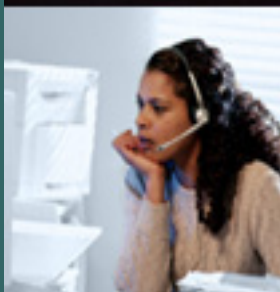
Performance/Troubleshooting (NAM-1/2)

Performance/Troubleshooting (NM-NAM)

QoS Monitoring

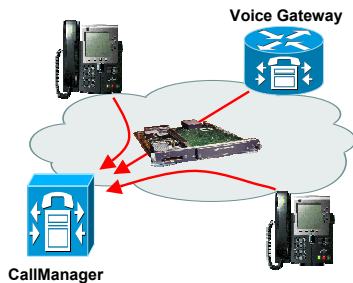
VoIP Monitoring

Trend Analysis



Scenario 4

VoIP Monitoring



- **Enable Voice Monitoring**
- **Control Protocol Statistics**
- **Phone Statistics**
 - All Calls
 - Individual Call
- **Active Call Statistics**

NAM gathers statistics based on SCCP, H.323, MGCP, and SIP messages.

Scenario 4 - VoIP Monitoring

The NAM can collect the control and diagnostic messages sent from IP phones to the Cisco Call Manager application and provide network engineers with valuable information about the voice aspects of a network. Because Dean has configured the Catalyst 6500 Series NAM to SPAN the port connected to the Cisco Call Manager application, he will be able to collect all traffic from IP phones located in the various workgroup access switches to the Cisco Call Manager. It is important to note that to use the voice monitoring feature of the NAM, you must SPAN a port or VLAN that will contain the Cisco Call Manager traffic. Also, the Cisco Call Manager must have “Call Diagnostics Recording” enabled for IP phones to send diagnostic statistics to the Cisco Call Manager.

Scenario 4

Enable VoIP Monitoring

Enable

Setup > Monitor > Voice Monitoring

	SCCP	H.323	MGCP	SIP
Monitoring Enabled:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number of phone table rows (10-1000):	300	200	200	200
Number of call table rows (10-1000):	300	200	200	200
Number of top packet jitter rows (1-20):	5	5	5	5
Number of top packet loss rows (1-20):	5	5	5	5
Debug:	<input type="checkbox"/>			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				

VoIP monitoring is enabled for all traffic and not by individual VLANs

Enable VoIP Monitoring

Like all other NAM monitoring features, voice monitoring must be enabled before any data collection will take place. Enabling voice monitoring differs from enabling the other monitoring features because voice is either enabled or not, whereas other collections are enabled on a per-data source basis.

To enable voice monitoring, Dean does the following:

- Step 1. Select **Setup > Monitor > Voice Monitoring**. The Voice Monitor Setup screen is displayed.
- Step 2. Voice monitoring on the NAM is performed by decoding the information found in SCCP, H.323, MGCP, or SIP control messages. To enable any of them, simply check the appropriate Monitoring Enabled checkbox. You can also decide on the number of entries in the various voice reports to help conserve NAM resources.
- Step 3. Click **Apply** to begin voice monitoring activities.

Note: For advanced troubleshooting, the Debug checkbox can be selected to include calls in all phases, including call setup.

Dean is now ready to look at the voice services that Q-Bits converged network offers.

Scenario 4

Voice Overview

Monitor > Voice/Video > Voice Overview

To View Calls with "Worst" Packet Loss and Jitter

Aggregate Statistics						
	Protocol	Calls Monitored	Avg Pkt Loss (%)	Avg Jitter (ms)	Worst Pkt Loss (%)	Worst Jitter (ms)
<input checked="" type="radio"/>	SCCP	3 K	0.0200	0	0.6900	0
<input type="radio"/>	H.323	10	-	-	-	-
<input type="radio"/>	MGCP	0	-	-	-	-
<input type="radio"/>	SIP	15	-	-	-	-
↑--Select a protocol then take an action-->						Details

Voice Overview

Dean first chooses to view the Voice Overview report that shows him the overall health of the voice network. The Voice Overview report details the number of calls monitored and the average and worst percentage of packet loss and jitter. A sub-report can then be viewed to show the top five calls with the worst jitter and the top five calls with the worst packet loss. If he wants to, Dean can reconfigure the number of calls in the "worst" list from 1 to 20 from the Voice Monitor Setup screen. The Voice Overview report provides Dean with an excellent starting point for troubleshooting voice problems because it can pinpoint a single phone, a subnet of phones, or all phones.

To view the Voice Overview report:

Step 1. Select **Monitor > Voice > Voice Overview**. The Voice Overview report is displayed.

Based on this report, Dean concludes that the quality of the voice network is good because there is very little packet loss and no jitter. If problems were indicated, Dean could choose to view the five worst calls for jitter and packet loss by doing the following:

Step 2. Highlight the protocol to see the five worst calls, and select **Details** (see next page).

Scenario 4

List of “Worst” Calls

Packet Loss - Worst Quality SCCP Calls									
	Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter
<input type="radio"/>	33001	6022642001	John Johnson	-	Tue May 21, 2005 12:45:20 PM	10.1.2.100	10.1.6.101	0.6900	0
<input checked="" type="radio"/>	34002	32001	Les More	Susie Banshee	Mon May 20, 2005 04:39:25 PM	10.1.4.102	192.168.76.41	0.0100	0
<input type="radio"/>	41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/>	41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/>	33001	6022641001	John Johnson	-	Tue May 21, 2005 12:45:43 PM	10.1.2.100	10.1.6.101	0.0000	0

↑-- Select an item then take an action -->

To view call details

Details

Clear

Jitter - Worst Quality SCCP Calls									
	Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter
<input type="radio"/>	41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/>	41001	33001	-	John Johnson	Tue May 21, 2005 12:49:12 PM	192.168.79.135	10.1.2.100	0.0000	0
<input type="radio"/>	33001	6022641001	John Johnson	-	Tue May 21, 2005 12:45:43 PM	10.1.2.100	10.1.6.101	0.0000	0
<input type="radio"/>	33001	6022642001	John Johnson	-	Tue May 21, 2005 12:45:20 PM	10.1.2.100	10.1.6.101	0.6900	0
<input type="radio"/>	33001	9192959001	John Johnson	-	Tue May 21, 2005 12:43:48 PM	10.1.2.100	10.1.6.101	0.0000	0

↑-- Select an item then take an action -->

Calls with “Worst” Packet Loss and Jitter

Details

Clear

List of “Worst” Calls

A separate window is opened containing two tables: the first shows the five calls with the worst packet loss and the second contains the five calls with the worst jitter. The calls listed as the “worst” include calls made since voice monitoring was enabled or the table was cleared. To restart the tracking of “worst” calls, select the **Clear** button.

To see the actual details for a listed call, highlight the call and click the **Details** button. (See next page.)

Scenario 4

Individual Call Statistics

Current Data: as of Wed 13 Sep 2006, 13:48:11 PDT

SCCP call detail for calling party		
	Calling Party	Called Party
Number:	34002	32001
IP Address:	10.1.4.102	192.168.76.41
Call Reference:	17416680	
Owner:	Les More	Susie Banshee
Call State:	On Hook	
RTP Port:	22588	20128
Line Instance:	1	
Conference Id:	0	
Pass Thru Party Id:	4722929	
RTP Sampling Period:	20	
Payload Type:	G.711 ulaw 64k	
RTP Pre Value:	11	
Silence Sup:	Off	
Max Frames per Pkt:	0	
G.723 Bit Rate:	-	
Start Time:	Thu 28 Jul 2005, 22:36:43 UTC	
End Time:	Thu 28 Jul 2005, 22:36:43 UTC	
Packets Sent:	25580	
Packets Received:	25577	
Octets Sent:	4399760	
Octets Received:	4399244	
Packet Loss (%):	0.0100	
Jitter (msec):	0	
Switch Port:	-	

Close

Details for
selected call

Individual Call Statistics

The Individual Call Statistics report also opens in a new browser window. Dean now has all known details about a particular call. The Traffic Analyzer gives Dean an incredible amount of detailed information about the calls that traversed his network, making post-call troubleshooting that much easier.

This report can be reached as a drill down from the “Known Phones” report as well.

Though the voice network is in good shape, Dean wants to look at other voice displays to understand how they will help him debug voice issues in the future.

Scenario 4

Overview of All Phones

The screenshot shows the NAM Traffic Analyzer interface. The 'Monitor' tab is selected, and the 'Known Phones' report is displayed. The report shows a list of phones with columns for Phone, IP Address, Name, Calls Monitored, Avg Pkt Loss %, and Avg Jitter (ms). A red arrow points from the call number '4' in the 'Calls Monitored' column to a yellow callout box that says 'Click to View all Calls to/from This Number'. Another yellow callout box says 'List of All Phones Seen'.

Phone	IP Address	Name	Calls Monitored	Avg Pkt Loss %	Avg Jitter (ms)
1. 32001	192.168.76.41	Susie Banshee	4	0.0000	0
2. 33001	10.1.2.100	John Johnson	5	0.0000	0
3. 34001	10.1.4.103	Joe Jones	4	0.0000	0
4. 34002	10.1.4.102	Les More	5	0.0000	0
5. 34999	192.168.76.58	Steven Schleimer	4	-	-
6. 42001	192.168.79.115	Mary Marian	4	-	-
7. 52001	192.168.79.124	-	3	-	-
8. 59001	192.168.79.125	-	1	-	-
9. 61001	192.168.79.84	Ralph Spoilsport	3	-	-
10. 72001	192.168.79.36	Willy Wonka	4	-	-

Overview of All Phones

The NAM voice monitoring features give Dean the ability to view statistics of each phone and, if necessary, drill down into each call to or from a phone and review quality statistics on a per-call basis. To view average quality statistics (packet loss and jitter) for each phone seen by the NAM, Dean does the following:

Step 1. Select **Monitor > Voice > Known Phones**. The Phones report is displayed.

Dean can now sort the list based on any of the columns and quickly look for phones experiencing high rates of either packet loss or jitter. To find out if that phone is experiencing poor quality for all calls or calls only to a certain phone or location, Dean does the following:

Step 2. Click the Phone you wish to get more details about (see next page).

Scenario 4

Listing of All Calls for Individual Phone

Current Data: as of Wed 13 Sep 2006, 20:09:52 UTC

Phone Details	
Phone:	34002
Name:	Les More
IP Address:	10.1.4.102
Switch Port:	-
Protocol:	SCCP

Aggregate Statistics	
Calls Monitored:	5
Average Packet Loss (%):	0.0000
Average Jitter (msec):	0
Worst Packet Loss (%):	0.0100
Worst Jitter (msec):	0

Last Five Calls to or from This Number

Last 5 Calls									
	Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Address	Called IP Address	% Pkt Loss	Jitter (msec)
<input type="radio"/>	34002	32001	Les More	Susie Banshee	Mon May 20, 2005 04:39:25 PM	10.1.4.102	192.168.76.41	0.0100	0
<input type="radio"/>	34002	32001	Les More	Susie Banshee	Mon May 20, 2005 04:35:29 PM	10.1.4.102	192.168.76.41	0.0000	0
<input type="radio"/>	61001	34002	Ralph Spoilsport	Les More	Mon May 20, 2005 04:27:53 PM	192.168.79.84	10.1.4.102	0.0000	0
<input type="radio"/>	33001	34002	John Johnson	Les More	Mon May 20, 2005 04:27:41 PM	10.1.2.100	10.1.4.102	0.0000	0
<input type="radio"/>	61001	34002	Ralph Spoilsport	Les More	Mon May 20, 2005 04:26:23 PM	192.168.79.84	10.1.4.102	0.0000	0

←-- Select a call, then take an action -->

To View Call Details

[Details](#)

[Close](#)

Listing of All Calls for Individual Phone

A new window opens with call-quality statistics for the selected phone and the last five calls to or from this number. Dean uses this screen to determine the extent of the quality problems for a particular phone. To get even more details about a particular call, Dean does the following:

- Step 1. Select the radio button next to the call of interest and then select **Details**. The Individual Call Statistics Report is displayed in a new browser window. This report is the same as the one shown earlier.

Scenario 4

Listing of Active Calls

The screenshot shows the Cisco NAM Traffic Analyzer web interface. The top navigation bar includes 'Setup', 'Monitor', 'Reports', 'Capture', 'Alarms', and 'Admin'. The 'Monitor' tab is selected, and the 'Voice/Video' section is active. The 'Active Calls' page is displayed, showing a table of active calls. A red arrow points to the 'Caller Number' column header, with a callout box that says 'Click to view call details'.

	Caller Number	Called Number	Caller	Called	Time of Call	Caller IP Addr	Called IP Addr
1.	33001	34001	John Johnson	Joe Jones	Mon May 20, 2005 04:50:53 PM	10.1.2.100	10.1.4.103
2.	24999	32001	Steven Schleimer	Susie Banshee	Mon May 20, 2005 04:51:33 PM	192.168.76.58	192.168.76.41
3.	42001	52001	Mary Marian	-	Mon May 20, 2005 04:51:23 PM	192.168.79.115	192.168.79.124
4.	59001	72001	-	Willy Wonka	Mon May 20, 2005 04:51:15 PM	192.168.79.125	192.168.79.36
5.	61001	34002	Ralph Spoilsport	Les More	Mon May 20, 2005 04:51:02 PM	192.168.79.84	10.1.4.102

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-53

Listing of Active Calls

Dean has now looked at his options for analyzing completed calls, but what about calls in progress? The NAM can provide information about active calls as well (but remember that most information is retrieved at the end of the call when statistics are passed from the phone to the Cisco Call Manager.)

To see which phones are actively involved in a current call, Dean does the following:

Step 1. Select **Monitor > Voice > Active Calls**. The Active Calls report is displayed.

Dean can see all calls currently in progress. Notice that the only information available at this time are the call endpoints (phone numbers, usernames, and IP addresses) and the time the call was initiated. A few more details about any call, such as the Real-Time Protocol (RTP) port used, can be viewed by doing the following:

Step 2. Click the Caller Number of the active call to view more details. (See next page.)

Scenario 4

Individual Active Call Details

Current Data: as of Wed 13 Sep 2006, 13:48:11 PDT

SCCP call detail		
	Calling Party	Called Party
Number:	33001	34001
IP Address:	10.1.2.100	10.1.4.103
Call Reference:	17417052	17417053
Owner:	John Johnson	Joe Jones
Call State:	Connect	Connect
RTP Port:	27416	20278
Line Instance:	1	1
Conference Id:	0	0
Pass Thru Party Id:	4725937	4725953
RTP Sampling Period:	20	20
Payload Type:	G.711 ulaw 64k	G.711 ulaw 64k
RTP PRE Value:	11	11
Silence Sup:	Off	Off
Max Frames per Pkt:	0	0
G.723 Bit Rate:	-	-
Start Time:	Thu 28 Jul 2005, 22:36:43 UTC	
Packets Sent:	Thu 28 Jul 2005, 22:36:43 UTC	
Packets Received:	-	-
Octets Sent:	-	-
Octets Received:	-	-
Packet Loss (%):	-	-
Jitter (msec):	-	-
Switch Port:	-	-

Close

Details for Selected Active Call

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-54

Individual Active Call Details

Again, many of the details about a call will not be available until after the call has been completed. However, some of the information on this screen provides Dean with clues as to where to begin troubleshooting. For example, if the phone switch port is listed, Dean could check its utilization to see if voice quality is poor because of high utilization on the port.

Dean is really excited. He was worried about voice services on the new network, but by using the NAM, he now knows that he has successfully transitioned to a high-performing, converged network.

CISCO SYSTEMS



Performance/Troubleshooting (NAM-1/2)

Performance/Troubleshooting (NM-NAM)

QoS Monitoring

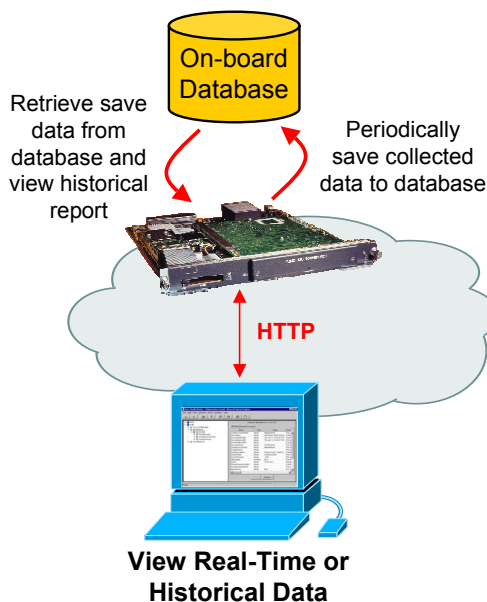
VoIP Monitoring

Trend Analysis



Scenario 5

Trend Analysis



- **Real-Time Trend**
- **Configure Basic Reports**
 - Port Statistics
 - Application Statistics
- **View Basic Reports**

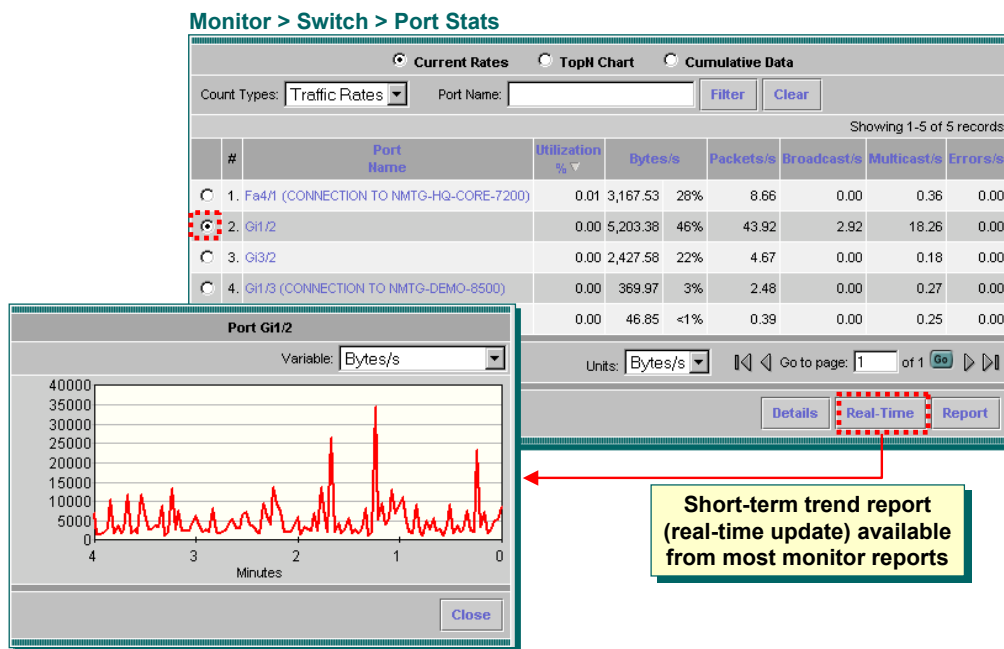
Scenario 5 - Trend Analysis Example

The data provided by the NAM will make Dean's life easier for real-time analysis and troubleshooting. But wouldn't it also be great to collect this data over time for trend analysis or historical reporting? All that is needed is a database to store data collected by the NAM at regular intervals and then run reports on the data over time. Well the NAM has this feature, allowing you to configure data collection to a database for up to 100 days!

Of course to gather data long term, the user must remember that if the SPAN, VACL, or NDE (Internal, External, NDE on NM-NAM) data source containing the traffic you want to trend changes, then data can no longer be collected to the database. Dean wants to view long term how much of the total link usage is associated with Doom and Q-Bits Database development traffic. Let's see how Dean creates historical reports to trend the total byte rate of port Gi1/2 (currently spanned), and the byte rates of Doom and QbitsDB traffic on VLAN 130.

Scenario 5

Real-Time Trend Report



Real-Time Trend Report

Dean can always use basic monitoring reports to view a snapshot of the current application, host, and conversation traffic rates per port. He can also track them in real-time to get a view of how they are performing continuously over time. To view port Gi1/2 byte rate in a continuous manner, as opposed to a snapshot value, Dean uses the following steps:

Step 1. Select **Monitor > Switch > Port Stats**. The Port Statistics report is displayed.

Step 2. Select the radio button to the left of port Gi1/2, and click the **Real-Time** button. A new window is opened and begins tracking the byte rate of port Gi1/2.

Dean can use this short-term trend report to get an idea of how consistent the link attached to the port is running. For a longer term view of port Gi1/2 byte rate and to compare how much of that traffic is associated to certain applications, Dean needs to configure historical reports. Once created, the NAM will log the requested data to a database, and display all data together at a later time.

Scenario 5

Create Basic Report – Port Statistics

Reports > Basic Reports

Basic Report Type: All Types

Name	Type	Data Source	Interval	Create Time	Last Status
Select item(s) then take an action -->					
<div>Create View Rename Disable Enable Delete</div>					

Use the Reports tab to create long-term (100 days) historical trend reports

Select Report Type

Report Type:

- Applications
- Application Groups
- Hosts
- Conversations
- VLANs
- DiffServ
- Response Time
- Switch Ports
- Switch Health
- MPLS

Step 1 of 2 -

< Back Next > Finish Cancel

Setup Report Parameters

Port Information

☒ Switch Module: WS-X6408-GBIC

Port: Gi1/2

☐ Top N Ports

Report Settings

Report Name: Port Gi1/2-Bytes/sec ☒ Customized

Data Type: Bytes/sec

Polling Interval: 15 minutes

Step 2 of 2 -

< Back Next > Finish Cancel

Bytes/sec
Packets/sec
Utilization %
Broadcast Bytes/sec
Multicast Bytes/sec
Drop Events/sec

Create Basic Report – Port Statistics

Dean uses the following steps to create a basic historical report to help him trend the byte rate of port Gi1/2:

- Step 1. Select **Reports > Basic Reports**. A list of all the currently created basic reports and their status will be displayed. Dean's list is empty since he hasn't created any yet.
- Step 2. Select the **Create** button. The Select Report Type dialog is displayed (first screen of a two part wizard).
- Step 3. Select **Switch Port Statistics** report type and click the **Next>** button. The Setup Report Parameters dialog is displayed (step two of the wizard).
- Step 4. Select module 1 and port Gi1/2, click the **Customized** button to edit the report title. Choose **Bytes/Sec** as the value to log and graph and use the default logging interval of 15 minutes. Click the **Finish** button to create the report.

Dean could use this same procedure to create two Application Protocols reports to log the Doom and QbitsDB applications, but let's look at another way to create these reports.

Scenario 5

Quick Create Basic Report – Application

Monitor > Apps > Individual Applications

☒ Current Rates ☐ TopN Chart ☐ Cumulative Data

Data Source: Protocol:

Showing 1-5 of 162 records

#	Protocol	Packets/s	Bytes/s
<input type="radio"/> 1.	QbitsDB	1768.32	858759.98
<input checked="" type="radio"/> 2.	doom	923.43	84957.00
<input type="radio"/> 3.	snmp	13.70	4488.11
<input type="radio"/> 4.	others	26.82	1879.01
<input type="radio"/> 5.	icmp	9.78	1007.48

Rows per page: Go to page: of 33

Select an item then take an action -->

Quickly create historical reports from most monitor reports

Waiting for first data collection based on set polling interval

Clicking Reports takes you to the Reports > Basic Reports screen

Basic Report Type:

	Name	Type	Data Source	Interval	Create Time	Last Status
<input type="checkbox"/>	DOOM (VLAN 130)	Appl Protocol - Bytes/sec	VLAN 130	15 min	15 Jun 2005, 22:09:02	Pending
<input type="checkbox"/>	Port G1/2-Bytes/sec	Switch Port - Bytes/sec	Supervisor	15 min	15 Jun 2005, 22:08:29	Pending

Select item(s) then take an action -->

Quick Create Basic Report – Application

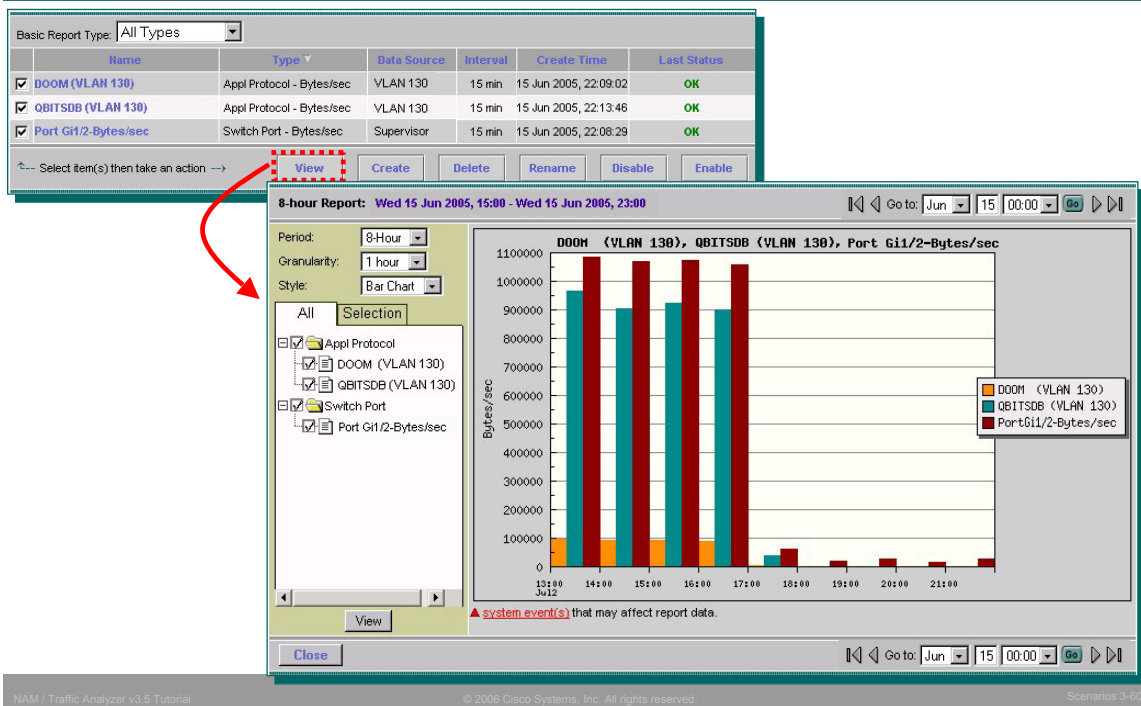
To create the two basic reports for tracking Doom and QbitsDB application traffic, Dean chooses to use the short-cut for creating basic reports:

- Step 1. Select **Monitor > Apps > Individual Applications** and **VLAN 130** from the Data Source pull-down menu. The Applications report is displayed.
- Step 2. Highlight the radio button next to the application to create a report for. In this case, Dean starts with the Doom application.
- Step 3. Click the **Report** button to create the basic report (albeit with default parameters). A dialog will appear informing you that this report does not exist and ask if you really want to create it. Click **OK**. The Basic Reports window (**Reports > Basic Reports**) is displayed showing the newly created report.

Dean repeats this procedure to create an Application Protocol report for the QbitsDB application.

Scenario 5

View Basic Reports



View Basic Reports

The data for the reports generated are being logged every 15 minutes. Some time later Dean uses the following steps to view the three values together to determine how much of the link is being consumed by these two protocols:

- Step 1. Select **Reports > Basic Reports**. The list of Basic Reports is displayed.
- Step 2. Click all three basic reports to view them on the same graph, and click **View**. A new window opens showing the data collected for the three reports.

Dean can quickly see that most of the link is utilized by these two protocols, especially the Q-Bits development effort. Dean can use this GUI to change the graphical display, or even the reports being displayed (if others were generated).

Scenario 5

Create Top N Reports

Reports > Basic Reports

The screenshot shows the 'Basic Report Type' dropdown set to 'All Types'. Below it is a table with columns: Name, Type, Data Source, Interval, Create Time, and Last Status. The 'Create' button is highlighted with a red dashed box. A red arrow points from the 'Create' button to the 'Select Report Type' dialog. In this dialog, 'Applications' is selected in the list. The 'Next >' button is also highlighted with a red dashed box. A red arrow points from the 'Next >' button to the 'Setup Report Parameters' dialog. In this dialog, the 'Top N Applications' radio button is selected and circled in red. The 'Report Name' is 'Top Applications - Bytes', 'Data Type' is 'Bytes/sec', 'Polling Interval' is '15 minutes', and 'Data Source' is 'Internal'. The 'Finish' button is highlighted with a red dashed box. A yellow callout box titled 'Top N Reports:' lists: Applications, Hosts, Conversations, Ports (NAM-1/2), Interfaces (NM-NAM), and MPLS (NAM-1/2). Another yellow callout box titled 'Default Name' points to the 'Report Name' field. A third yellow callout box titled 'Choose the appropriate Data Source' points to the 'Data Source' dropdown.

Create Top N Reports

The WAN link is an important asset for Q-bits and Dean wants to track general application usage across it. Rather than create a basic report for each application, Dean can create a basic report to display the top applications over the selected time period. Dean uses the following steps to create a basic historical report to help him trend the Top applications over time on the WAN link (earlier Dean used CEF to forward the WAN packets to the internal NM-NAM interface):

- Step 1. Select **Reports > Basic Reports**. A list of all the currently created basic reports and their status will be displayed. Dean's list is empty since he hasn't created any yet.
- Step 2. Select the **Create** button. The Select Report Type dialog is displayed (first screen of a two part wizard).
- Step 3. Select **Applications** report type and click the **Next>** button. The Setup Report Parameters dialog is displayed (step two of the wizard).
- Step 4. Select the **Top N Applications** radio button. Dean decides to use the default report name, chooses **Bytes/Sec** as the value to log and graph, the default logging interval of 15 minutes, and selects Internal as the Data Source. Click the **Finish** button to create the report.

Scenario 5

View Top N Reports

Narrow the types of reports displayed

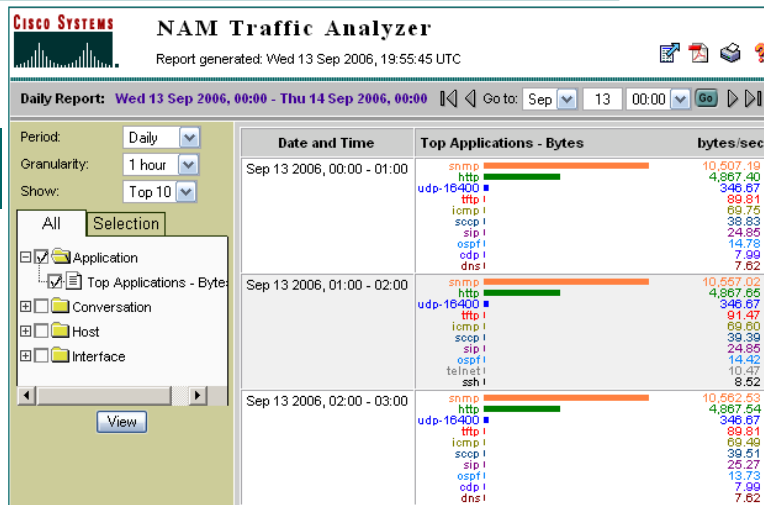
Type: Applications Data Source: Filter 0.3 GB allocated report data 10.8 GB available disk space

Name	Type	Data Source	Interval	Create Time	Last Status
<input checked="" type="checkbox"/> Top Applications - Bytes	Applications - Bytes/sec	Internal	15 min	29 Jun 2006, 01:08	OK

Select item(s) then take an action -->

Create View Rename Disable Enable Delete

Top 10 applications for each hour for one day



NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

Scenarios 3-62

View Top N Reports

The data for the report are being logged every 15 minutes. Some time later Dean uses the following steps to view the top applications on the WAN link:

- Step 1. Select **Reports > Basic Reports**. The list of Basic Reports is displayed.
- Step 2. Click the Top N report created, and click **View**. A new window opens showing the data collected.

Dean can quickly see the applications that are utilizing most of the bandwidth over time. If desired, Dean can change the granularity and the overall time period.

Dean is now confident in the use of his new network tool and its ability to provide him with the necessary metrics to troubleshoot the network, verify network implementation, and plan for future network growth.



Thank You!

Continue on to Chapter 4 to learn about some of the administrative tasks not yet discussed.

This page intentionally left blank.



NAM System Administration

Chapter 4

- **Cisco Network Analysis Modules (NAM)
NAM-1, NAM-2, and the NM-NAM**
- **Cisco NAM Traffic Analyzer Software v3.5**



Chapter 4 Outline

- **Requirements**
 - Hosting Hardware and Software
 - Client (Access to the NAM)
- **Administration**
 - Install
 - Initial Configuration
- **Maintenance**
- **Diagnostics & Troubleshooting Tips**



Chapter 4 Outline

This chapter provides highlights and important facts for installing, administering, and maintaining the different models of the Network Analysis Modules (the Cisco Catalyst 6500 series and Cisco 7600 series NAM-1, NAM-2, and the Cisco Branch Routers Series NM-NAM). This chapter also provides some quick command line tips for troubleshooting.

The information provided in this chapter is intended to give you an overview of the installation, maintenance, and troubleshooting of the NAM hardware to help in deployment planning. The reader should refer to the appropriate installation guide and release notes for exact details. Additional troubleshooting tips can also be found in the *NAM User Guide*.

The Administration section of this chapter, which covers installation and initial configuration, is actually presented as two parts – one for NAM-1, NAM-2 and one for the NM-NAM.

A Cisco.com link to the installation and user guides can be found in Chapter 5 of this tutorial.

Note(s):

- *Cisco Catalyst® 6500 and Cisco 7600 Series Network Analysis Modules will be referred to, in this tutorial, as the Cat6500 NAM(s), NAM-1, NAM-2 or NAM-1/2.*
- *Cisco Branch Routers Series NAM will be referred to, in this tutorial, as the NM-NAM.*
- *The term NAM refers to all modules, NAM-1, NAM-2, and the NM-NAM.*

CISCO SYSTEMS



➤ Requirements

- Administration
- Maintenance
- Diagnostics & Troubleshooting Tips



Requirements

NAM Specifications

	NAM-1	NAM-2	NM-NAM
Supported Platforms	Cat 6000/6500 Switches, Cisco 7600 Router	Cat 6000/6500 Switches, Cisco 7600 Router	2600XM, 2800, 3660, 3700, 3800 Series Routers
Operating System	CatOS / IOS (See next page for details)	CatOS / IOS (See next page for details)	IOS 12.3(7)T or later or IOS 12.4(1) or later
Typical Applications	Distribution, access, small core, branch office	Large core/distribution, server farm, data center	Branch Office WAN Access
Monitoring Interfaces	(2) 1 - SPAN/VACL 1 - NDE	(3) 2 - SPAN/VACL 1 - NDE	(2) 1 - CEF (WAN, LAN, NDE) 1 - FE (LAN, NDE)
RAM	512 MB	1 GB	256 MB
HDD	20 GB	20 GB	20 GB
Capture Buffers	125 MB	300 MB	70 MB

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

System Admin 4-4

NAM Specifications

The NAM software image v3.5 is compatible with the NAM hardware modules for the Catalyst 6500 and Cisco 7600 Series and the Cisco Branch Routers Series, illustrated above. This tutorial covers aspects of both types of NAMs – the NAM-1, NAM-2 and the NM-NAM.

The NAM hardware, for the most part, is transparent to the end user. Hardware wise, what matters most to the end-user is the number of monitoring interfaces and the types of data sources they support, and the amount of CPU and memory which provides increased monitoring resources and flexibility.

This chart depicts some of the key hardware differences and uses of the various NAM modules.

Note(s):

- The NAM 3.5.1a version has been tested with IOS 12.4(10).

Requirements

NAM-1, NAM-2 Host Platform Hardware/Software Details

Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

Cisco IOS	
Software Version	Hardware
Release 12.1(13)E or later	Supervisor Engine 2 with an MSFC2
Release 12.2(14)SX1 or later	WS-SUP720
Release 12.2(18)SXF or later	WS-SUP32

* Refer to notes for specific IOS requirements for the **Virtual SPAN** and **ERSPAN** features

Catalyst OS	
Software Version	Hardware
Release 7.3(1) or later	Supervisor Engine 2
Release 8.2(1) or later	WS-SUP720

NAM-1, NAM-2 Host Hardware and Software Requirement Details

The charts indicates the correct Cisco Catalyst operating system software version and Supervisor Engine combination for using either the NAM-1 or NAM-2.

The Network Analysis Module can be installed in the Catalyst 6500 series and Cisco 7600 series family chassis. The hosting device must have the specified hardware and software version as illustrated above

The Cisco CatOS Switch requires no additional configuration in order to host the NAM other than the hardware and software requirements just discussed. However, every Cisco Catalyst switch is capable of gathering a subset of Remote Monitoring (RMON) statistics on a per-port basis—known as mini-RMON (Layer 2 statistics, history of those statistics, alarms, and events). Typically, these statistics are used to provide general port status and health. To utilize this capability, you must define the switch Simple Network Management Protocol (SNMP) community strings to enable data collection by the NAM (and/or a third-party management application).

Remember, if you need more data than mini-RMON offers in order to resolve a problem, you can also SPAN the traffic on any port to the NAM monitor port for full RMON analysis.

Note(s):

- *Cisco IP Phone firmware 6.0 and above is required for SIP voice packet quality monitoring*
- *IOS 12.2(18)SXD or CatOS 8.5, at minimum, are required to support the **Virtual SPAN** feature.*
- *IOS 12.2(18)SXE4, at minimum, is required to support the **ERSPAN** feature*
- *You should always consult the Release Notes included with the product for the most up-to-date hardware and software requirements.*

Requirements

Client (Access to the NAM's Web Server)

Browser	Version	Platform	Java Plug-in Support
Internet Explorer (recommended)	6.0 (or later)	Windows, XP Prof.	JRE Version 5.0 Update 6
Mozilla	1.7	Windows, XP Prof. Solaris	
Firefox	1.5	Windows, XP Prof. Solaris Linux (Redhat, SuSe)	

Although the Traffic Analyzer does not require a Java plug-in, one might be required to use a Java Virtual Machine (JVM)



Browser Configuration

- Enable Java and JavaScript
- Accept all cookies
- Check for newer versions of pages *every time it loads a page*
- Memory and disk cache size must be at least 6 MB

Web Browser Requirements

Client access to the NAM Traffic Analyzer software is via a standard web browser. Cisco has tested several browsers for compatibility with the NAM, illustrated above.

Although the Traffic Analyzer does not require a Java plug-in, one might be required to use a Java Virtual Machine (JVM). The above listed plug-ins have been tested for browsers that require a plug-in for JVM.

The browsers also require some configuration to work seamlessly with the NAM:

- Enable Java and Java Script
- Configure your browser to accept all cookies
- Configure your browser to check for newer versions of pages every time it loads a page
- Set your browser cache to at least 6 MB

Note(s):

- *It is always a good idea to check the latest release notes for up-to-date information regarding system requirements.*
- *Clients not conforming to the above requirements may also work but have not been tested and certified by Cisco and therefore will not be supported should problems arise.*

CISCO SYSTEMS



- Requirements
- **Administration**
 - **NAM-1, NAM-2**
 - NM-NAM
- Maintenance
- Diagnostics & Troubleshooting Tips



NAM-1, NAM-2 Administration

Install NAM Module



NAM module can occupy any slot, except Supervisor slot

Installing the NAM-1, NAM-2

When deployed properly, the capabilities of the NAM provide a wide array of benefits for analyzing data and voice streams. Chapter 2 discussed many of the issues you must consider when deciding how and where to deploy the NAM-1, NAM-2. Typical deployment spots include LAN aggregation points where it can collect the most data, service points (server farms, data centers, and so on) where performance is critical, and at important access points. Of course, actual placement depends on the problem you are trying to solve with the NAM.

Note: Placement and intended use may also dictate the need for the higher-performance NAM-2.

After you have identified the appropriate locations for the NAM, and you have determined that the Cisco Catalyst® Switch hosting the NAM meets all requirements, you can then install the NAM blade and configure it for basic management (for use with the Traffic Analyzer software embedded in the NAM or a third-party application), and for any additional monitoring, data source, or auto-start options.

The NAM can be installed in any slot on the host Cisco Catalyst® Switch except for the slot(s) that are reserved for the Supervisor module(s).

The NAM is a complex piece of electrical hardware and should be treated carefully. Installers should follow all safety precautions when handling and installing any electrical component to avoid damage. Follow all recommendations listed in the install guide to ensure the best operating environment for the NAM.

Note: The NAM must be properly shut down before removing it from the switch or serious damage to the NAM may occur. Consult the information later in this chapter (NAM Maintenance) prior to removing the NAM blade.

NAM-1, NAM-2 Administration

Verify the NAM Installation



Green - Operational
Red - Failure
Orange - Disabled/Shutdown/Running Tests

Check NAM Status LED

**Verify NAM detected by Supervisor
(show module)**

```
NMTG-HQ1-6509>show module
```

Mod	Ports	Card	Type	Model	Serial No.
1	6	Firewall Module		WS-SUC-FWM-1	SAD0918066R
2	16	16 port 1000mb GBIC ethernet		WS-X6416-GBIC	SAD05160429
3	48	48 port 10/100 mb RJ45		WS-X6348-RJ-45	SAD042600JJ
4	8	Network Analysis Module		WS-SUC-NAM-2	SAD09050D3L
5	8	T1		WS-X6608-T1	SAD05070JXN
6	2	Supervisor Engine 720 (Active)		WS-SUP720-3BXL	SAD082900ZF

Mod	MAC addresses	Hw	Fw	Sw	Status
1	0014.1cd5.9104 to 0014.1cd5.910b	3.0	Unknown	Unknown	PwrDeny
2	0002.7ef8.9294 to 0002.7ef8.92a3	1.2	5.4(2)	8.3(0.156)RO	Ok
3	0002.7ef3.d380 to 0002.7ef3.d3af	1.1	5.4(2)	8.3(0.156)RO	Ok
4	0003.3236.0404 to 0003.3236.040b	3.0	7.2(1)	3.5(1)	Ok
5	0003.3282.d898 to 0003.3282.d89f	1.1	Unknown	Unknown	PwrDown
6	0011.92e6.db90 to 0011.92e6.db93	4.0	8.1(3)	12.2(18)SXD	Ok

NAM / Traffic Analyzer v3.5 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

System Admin 4-9

Verifying the Installation (NAM-1, NAM-2)

Before proceeding with any configuration, you should verify that the NAM hardware is functioning properly and that the host switch recognizes the NAM you have installed. The Status LED on the NAM front panel provides basic status information. The status LED appears green when the hardware is functioning properly. An orange status indicates that the NAM is performing boot tests, it has been shut down, or it has been disabled. A red LED indicates failure. Upon first installation and power up, you may need to wait several minutes for the tests to complete and for the LED to turn green.

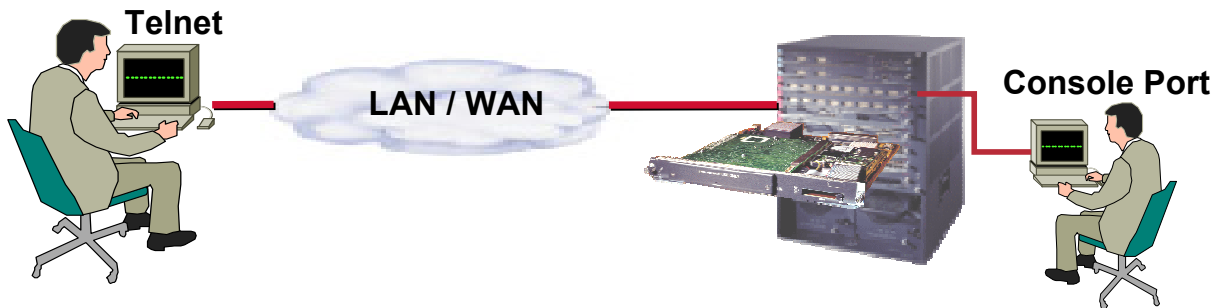
After you verify that the NAM is functioning properly, you may then want to verify that the switch recognizes the NAM. To verify this, use the `show module` command from the Cisco Catalyst CLI. The `show module` command generates output that indicates which slot the NAM is in as well as its status—ok, disabled, down, other (tests running), or failed. The output also indicates the version of software used by the NAM. Once the NAM is online, you can begin the initial setup of the NAM.

Note(s):

- To determine which image the NAM is using, you can use the `show module` command or session into the NAM. When using the application image, the `show module` output will indicate the software version being used by the NAM. If using the maintenance image, the software version number will not be the NAM release version and should be followed by an "m."

NAM-1, NAM-2 Administration

Initial Configuration – IP Settings



- Access CLI of hosting device (Telnet or Console Port)
- Establish console session to NAM module
- Login to NAM (default login: **root**, password: **root**)
- Enter IP configuration
 - IP Address, Subnet Mask , Broadcast Address
 - IP Hostname, Domain Name
 - Default Gateway
 - DNS Name Server (if applicable)
- Verify IP configuration

Configuring Initial Setup (NAM-1, NAM-2) – IP Settings

Like most network devices, the user must provide the NAM with an initial IP configuration to enable communication with other devices, whether for management purposes (Telnet) or for retrieving data.

To configure the IP settings, access the command line interface (CLI) of the hosting device using Telnet or through the console port and then session to the slot number where the NAM resides using the command below. The syntax differs slightly for Cisco IOS and CatOS devices.

```
CatOS Console# session [module_number]
```

```
IOS Console# session slot [slot_number] processor 1
```

The login prompt for the NAM CLI will be displayed. By default, the administrative login is *root*, with the password also set to *root*. It is important to change this password for security purposes by using the *password* command. The NAM banner message will indicate if the default password has not been changed.

Use the following syntax (on the next page), to enter the necessary IP settings listed above.

NAM-1, NAM-2 Administration

Initial Configuration – IP Settings

```
Console> (enable) session mod_num --- CatOS
```

```
Console> (enable) session slot slot_num processor 1 --- IOS
```

```
Root@localhost#      ip address ip-address subnet-mask  
                      ip broadcast broadcast-address  
                      ip host name  
                      ip gateway default-gateway  
                      ip domain domain-name  
                      ip nameserver ip-address [ip-address]
```

Configuring Initial Setup (NAM-1, NAM-2) – IP Settings, continue ...

To configure the IP address and subnet mask, enter:

```
root@localhost# ip address ip-address subnet-mask
```

To configure the IP broadcast address, enter:

```
root@localhost# ip broadcast broadcast-address
```

To configure the IP host name used in the CLI prompt, show commands, and log messages, enter:

```
root@localhost.localdomain# ip host [host-name]
```

To configure the default gateway, enter:

```
root@nam1.localdomain# ip gateway default-gateway
```

To configure the domain name for the NAM, enter:

```
root@localhost# ip domain domain-name
```

Optionally, configure one or more IP addresses as DNS name servers. This step is optional but highly recommended. Unexpected delays can occur if a name server is not set. To configure, enter:

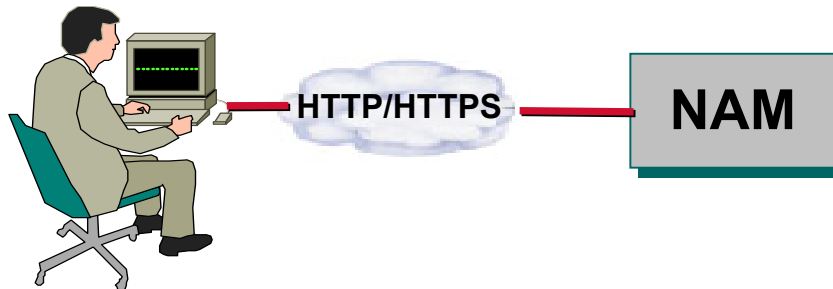
```
root@localhost.localdomain# ip nameserver ip-address
```

Verify the NAM IP configuration by entering:

```
root@localhost.localdomain# show ip
```


NAM-1, NAM-2 Administration

Initial Configuration – Enabling the Web Server



Before using NAM Traffic Analyzer software, first enable the web server on the NAM:

```
Root@localhost# ip http server enable
```

```
Enter a web username:
```

```
Enter a password:
```

You will be prompted for the web username and password when logging into the web interface of the NAM

Configuring Initial Setup (NAM-1, NAM-2) – Enabling the Web Server

After you configure the NAM with an IP address, you can then communicate with the NAM over the network. Before you can access the NAM through a web browser, you must enable the NAM's web server using the CLI. To enable the Web server, choose either HyperText Transfer Protocol (HTTP) or Secure HTTP (HTTPS) as the access protocol. By default, the HTTPS commands are disabled.

For HTTP, use the `ip http server enable` command.

For HTTPS, use the `ip http secure server enable` command.

Note: You can also select to run the server on a port other than TCP 80. If you change the HTTP port, you must restart the server. After entering the command to enable the server, you will then be queried for a Web administration username and password. This is the account information used to access the NAM Traffic Analyzer software via a browser. Remember that the CLI account for the NAM is not a Web account and cannot be used to access the NAM via a Web browser.

To enable the HTTP secure server, install a strong crypto patch. If you prefer to use SSH instead of Telnet, you also must install a strong crypto patch. To install a strong crypto patch, follow these steps:

Step 1 Download the patch from Cisco.com and publish the patch on an FTP server.

Step 2 Install the patch by entering:

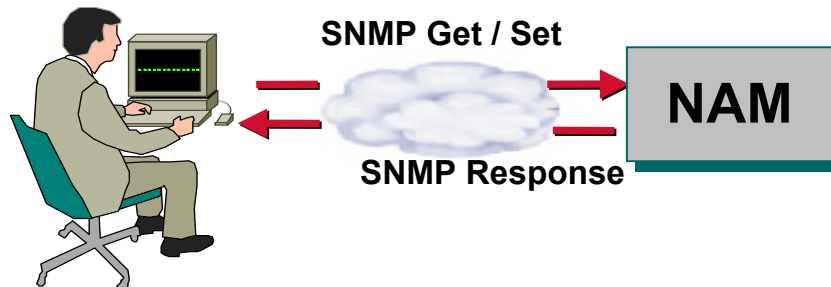
```
root@localhost# patch ftp-url
```

Where ftp-url is the FTP location and the name of the strong crypto patch.

Note: These steps are generic to all NAMs

NAM-1, NAM-2 Administration

Initial Configuration – SNMP Settings (Optional)



If you want to use an external network management application to communicate with NAM, first enable SNMP attributes:

- SNMP MIB variables (sysLocation, sysContact, sysName)
- Community strings (read-only, read-write)
- Can be done from CLI or via NAM web interface

Configuring Initial Setup (NAM-1, NAM-2) – SNMP Settings

The data collected and stored in the NAM can also be accessed using SNMP. Before retrieving any data from the NAM or setting any parameters on it, you must configure the NAM SNMP agent with community strings. Then you must also configure the monitoring application to use the same strings as you configured for the NAM in order to retrieve any data.

The community strings set for the NAM SNMP agent must be the same as the community strings of the host switch.

The SNMP parameters can be set via the NAM command line interface (CLI) or through the NAM web interface.

NAM-1, NAM-2 Administration

Initial Configuration – SNMP Settings (Optional)

Example shows how to configure a NAM running Catalyst OS

```
Root@localhost#      snmp location Location-string
                        snmp contact Contact-string
                        snmp name SysName-MIB-string
                        snmp community <string> ro
                        snmp community <string> rw
                        show snmp
```

Configuring Initial Setup (NAM-1, NAM-2) – SNMP Settings

To define the location of the NAM, enter:

```
root@localhost# snmp location <string>
```

To define a contact person for the NAM, enter:

```
root@localhost# snmp contact <string>
```

To define the SNMP read-only community string, enter:

```
root@localhost.localdomain# snmp community <string> ro
```

To define the SNMP read-write community string, enter:

```
root@localhost.localdomain# snmp community <string> rw
```

Verify the NAM SNMP settings by entering:

```
root@localhost.localdomain# show snmp
```

NAM-1, NAM-2 Administration

Initial Configuration – Management VLAN (Cisco IOS Only)

Note: Devices running Catalyst OS do not need to configure a VLAN as the NAM management port. The port is automatically synchronized to the VLAN assigned to interface sc0 on the Supervisor engine.

To select a VLAN for management, enter the configuration mode for the NAM and enter the following syntax at the command line:

```
analysis module [slot_number] management-port access-vlan  
[vlan_number]
```

```
Switch# configure terminal  
Enter configuration commands, one per line. End with  
CNTL/Z.  
  
Switch(config)#  
    analysis module 4 management-port access-vlan 5  
    exit  
Switch#
```

Configuring Initial Setup (NAM-1, NAM-2) – VLAN Settings

Configuring the Management VLAN is different depending on whether CatOS or IOS is used.

- For devices running Cisco IOS, you can change the NAM to any VLAN independent of the Supervisor. The NAM management port must be explicitly set to a VLAN. To configure a VLAN for the NAM management port on a Cisco IOS host, you must use the following command:

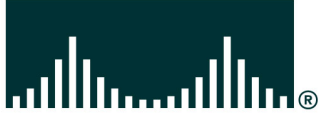
```
Console# analysis module [slot_num] management-port access-vlan [vlan_id]
```

- For devices running Catalyst OS, you do not need to configure a VLAN as the NAM management port. The port is automatically synchronized to the VLAN assigned to interface sc0 on the Supervisor engine. Therefore, ensure that the IP address for the NAM is in the same subnet/VLAN as sc0.

The NAM is now configured and ready to use for traffic monitoring!

This page intentionally left blank.

CISCO SYSTEMS

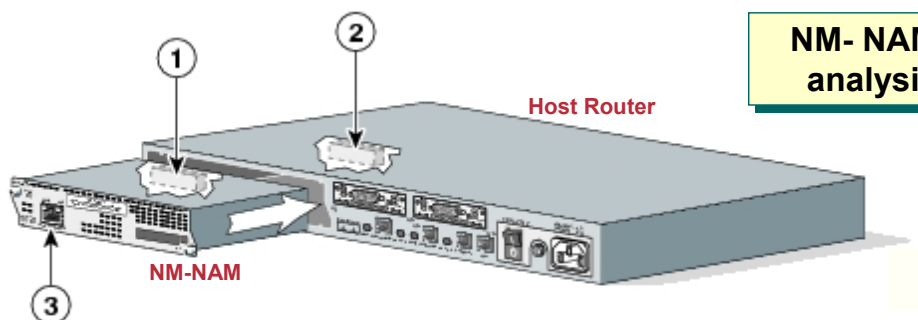


- Requirements
- **Administration**
 - NAM-1, NAM-2
 - **NM-NAM**
- Maintenance
- Diagnostics & Troubleshooting Tips



NM-NAM Administration

Install NAM Module



Interface	Interface type	Location	Configure and manage from
1 Internal NAM interface	Fast Ethernet	NM-NAM internal	NAM CLI
2 Analysis-Module interface	Fast Ethernet	Router internal	Cisco IOS CLI
3 External NAM interface	Fast Ethernet	NM-NAM faceplate	NAM CLI

Installing the NM-NAM

After you have identified the appropriate locations for the NM-NAM, and you have determined that the router hosting the NM-NAM meets all requirements, you can then install the NAM blade and configure it for basic management (for use with the Traffic Analyzer software embedded in the NAM or a third-party application), and for any additional monitoring, data source, or auto-start options.

The NM-NAM must be placed in the slot specifically used for a service module. Remember the NM-NAM is a complex piece of electrical hardware and should be treated carefully. Installers should follow all safety precautions when handling and installing any electrical component to avoid damage. Follow all recommendations listed in the install guide to ensure the best operating environment for the NAM.

Configuration of the NM-NAM is a little different than the NAM-1, NAM-2. Because the NM-NAM plugs into a router interface, that interface must first be configured using the router CLI. Next, as will be further discussed shortly, the IP address of the NM-NAM is applied to one of its two interfaces.

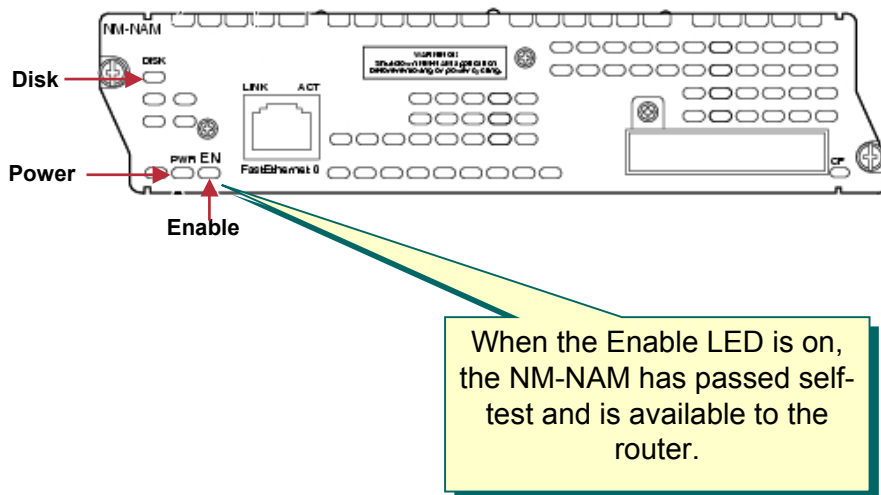
Note: Unlike other network modules, network analysis modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the network analysis module must be shut down in an orderly fashion before the network module is removed.

For more information on NM-NAM installation, see:

http://cco/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/nmnam.htm

NM-NAM Administration

Verify Installation



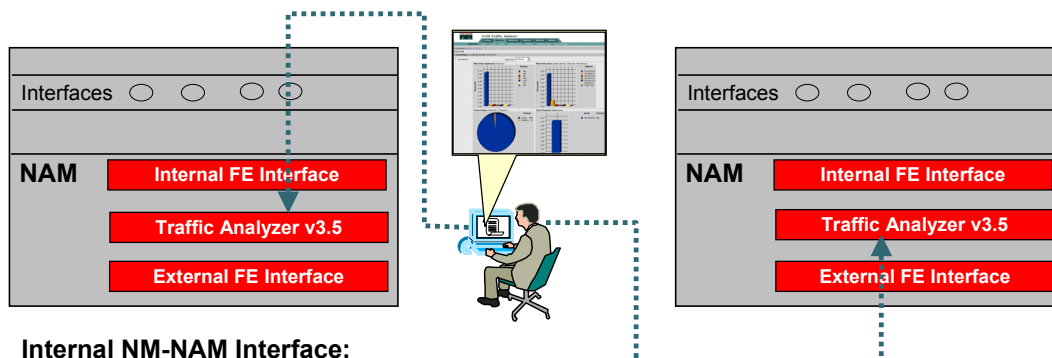
Verifying the Installation (NM-NAM)

Before proceeding with any configuration, you should verify that the NAM hardware is functioning properly. The NM-NAM has an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router.

NM-NAM Administration

NM-NAM Management Interface

Management Interface is used to communicate with Traffic Analyzer software (HTTP, SNMP). Which one you use, determines how to configure NAM IP.



Internal NM-NAM Interface:

- Use router CLI to assign an IP address from a routable subnet to the Analysis-Module interface
- For the NAM, use NAM CLI to assign an IP address from the same subnet that is assigned to the Analysis-Module interface.

External NM-NAM interface:

- Use router CLI to assign an IP address to the Analysis-Module interface. The subnet does not need to be routable.
- For the NAM, use NAM CLI to assign an IP address from the subnet that is connected to the external NAM interface.

NM-NAM Management Interface

To actually configure IP on the NM-NAM itself, the administrator must first decide which of the two NAM interfaces are to be used as the management interface or the interface end-user will use to communicate with the NM-NAM. (management traffic such as IP, HTTP, SNMP, Telnet, and SSH.) You cannot send management traffic through both NAM interfaces at the same time.

Note: Using the Internal NM-NAM interface as the management interface requires router resource. Using the External NM-NAM interface as the management interface requires the interface to be connected to a LAN.

How you assign IP addresses on the NAM network interfaces depends on which NAM interface, internal or external, you use for management traffic.

If you select the internal NAM interface to handle management traffic:

- For the Analysis-Module interface (in Cisco IOS CLI), assign an IP address from a routable subnet. To conserve IP address space, you can configure the Analysis-Module as an IP unnumbered interface and borrow the IP address of another router interface, such as a Fast Ethernet or loopback interface. The borrowed IP address must come from a routable subnet.
- For the NAM system (in NAM CLI), assign an IP address from the same subnet that is assigned to the Analysis-Module interface.

If you select the external NAM interface to handle management traffic:

- For the Analysis-Module interface (in Cisco IOS CLI), we recommend that you use the IP unnumbered interface configuration to borrow the IP address of another router interface. The subnet does not need to be routable.
- For the NAM system (in NAM CLI), assign an IP address from the subnet that is connected to the external NAM interface.

NM-NAM Administration

Router Analysis Module Interface Configuration

Configure Analysis-Module Interface

```
Router (config)# interface analysis-module slot/port
```

Set Analysis-Module Interface IP Address

/ If you use the ip unnumbered command, requires static requires static route if Internal NAM interface is the Management Interface */*

```
Router (config-if)# ip unnumbered FastEthernet slot/port
```

/ If you use a routable IP address and subnet mask */*

```
Router (config-if)# ip address ip_address netmask
```

Activate Analysis-Module Interface

```
Router (config-if)# no shutdown
```

Router Analysis Module Interface Configuration (NM-NAM)

The first step in configuring the NAM is to first configure the router's analysis module interface. Since all connected interfaces of a router require an IP address, and the analysis module interface is connected to the NM-NAM, the first step is to give the router's analysis module interface an IP address.

The above commands provide the basics for configuring the analysis module interface. If end-user are to communicate with the NAM through this interface then it must include a route to it.

Note(s):

- For the **ip unnumbered** command, make sure that a static route is configured on the router CLI for the NAM IP address that you configure through the NAM CLI. The following is a sample configuration:

```
ip route <nam-ip-address> 255.255.255.255 Analysis-Module slot/0
```

- On the NAM, the IP address must belong to the subnet of the parent interface for the Analysis-Module slot/0 (such as fa0/0). The NAM default gateway should be the parent interface IP.
- For a detailed explanation, see: *Configuring a Static Route to the NAM Through the Analysis-Module Interface* at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide09186a00801d6096.html#wp1046001

NM-NAM Administration

Initial Configuration – IP Settings

Session to NM-NAM

```
Router# service-module analysis-module slot/0 session
```

Select Management Interface

```
Root@localhost# ip interface {internal | external}
```

Enable Packet Monitoring on Interface

```
Root@localhost# analysis-module monitoring
```

IP Settings

```
Root@localhost# ip address ip-address subnet-mask
ip broadcast broadcast-address
ip host name
ip gateway default-gateway
ip domain domain-name
ip nameserver ip-address [ip-address]
```

Enable HTTP NAM Web Interface

```
Root@localhost# ip http server enable
```

Initial Configuration (NM-NAM) – IP Settings

To configure an IP address for the NM-NAM, first create a session to the NM-NAM by entering the exec-level command **service-module analysis-module slot/0 session**. The login prompt for the NM-NAM CLI will be displayed. By default, the administrative login is *root*, with the password also set to *root*. It is important to change this password for security purposes by using the *password* command.

Next, select the NM-NAM interface to use as the management interface, and enter the interface configuration mode: **ip interface {internal|external}**.

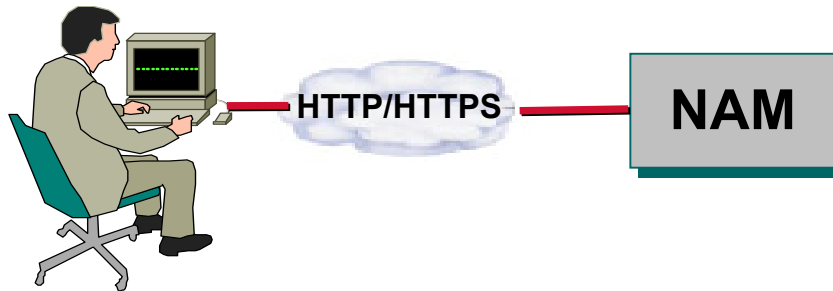
Now enter IP configuration commands much like you would on any interface.

Note(s):

- If configuring the Internal NM-NAM interface, the IP address must be in the same subnet as the Router's analysis module interface.
- If configuring the external NM-NAM interface, the IP address must be in the same subnet as the LAN it is connected to.
- If you wish to use both the internal and external interface for NAM analysis, make sure you enable it on both interfaces.

NM-NAM Administration

Initial Configuration – Enabling the Web Server



Before using NAM Traffic Analyzer Software, first enable the web server on the NAM:

```
Root@localhost# ip http server enable
```

```
Enter a web username: _____
```

```
Enter a password: _____
```

You will be prompted for the web username and password when logging into the web interface of the NAM

Configuring Initial Setup (NM-NAM) – Enabling the Web Server

After you configure the NAM with an IP address, you can then communicate with the NAM over the network. Before you can access the NAM through a web browser, you must enable the NAM's web server using the CLI. To enable the Web server, choose either HyperText Transfer Protocol (HTTP) or Secure HTTP (HTTPS) as the access protocol. By default, the HTTPS commands are disabled.

For HTTP, use the `ip http server enable` command.

For HTTPS, use the `ip http secure server enable` command.

Note: You can also select to run the server on a port other than TCP 80. If you change the HTTP port, you must restart the server. After entering the command to enable the server, you will then be queried for a Web administration username and password. This is the account information used to access the NAM Traffic Analyzer software via a browser. Remember that the CLI account for the NAM is not a Web account and cannot be used to access the NAM via a Web browser.

To enable the HTTP secure server, install a strong crypto patch. If you prefer to use SSH instead of Telnet, you also must install a strong crypto patch. To install a strong crypto patch, follow these steps:

Step 1 Download the patch from Cisco.com and publish the patch on an FTP server.

Step 2 Install the patch by entering:

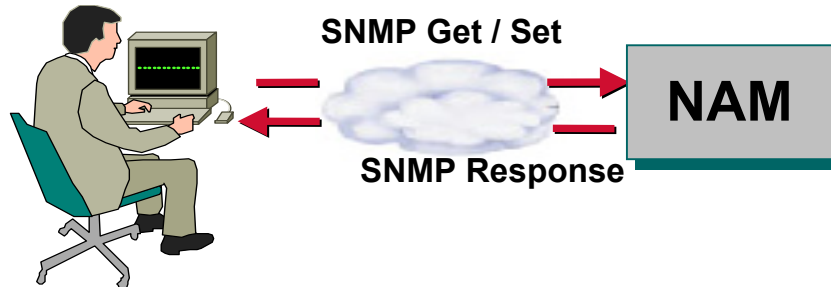
```
root@localhost# patch ftp-url
```

Where ftp-url is the FTP location and the name of the strong crypto patch.

Note: These steps are generic to all NAMs

NM-NAM Administration

Initial Configuration – SNMP Configuration (Optional)



If you want to use an external network management application to communicate with NAM, first enable SNMP attributes:

- SNMP MIB variables (sysLocation, sysContact, sysName)
- Community strings (read-only, read-write)
- Can be done from CLI or via NAM web interface

Configuring Initial Setup (NM-NAM) – SNMP Configuration

The data collected and stored in the NAM can also be accessed using other SNMP management. Before retrieving any data from the NAM or setting any parameters on it, you must configure the NAM SNMP agent with community strings. Then you must also configure the monitoring application to use the same strings as you configured for the NAM in order to retrieve any data.

The SNMP parameters can be set via the NAM CLI or through the NAM web interface.

The community strings set for the NAM SNMP agent must be the same as the community strings of the host switch. For example,

```
root@localhost.localdomain# snmp community community-string rw
root@localhost.localdomain# snmp community community-string ro
```

The NM-NAM is now configured and ready to use for traffic monitoring!

CISCO SYSTEMS

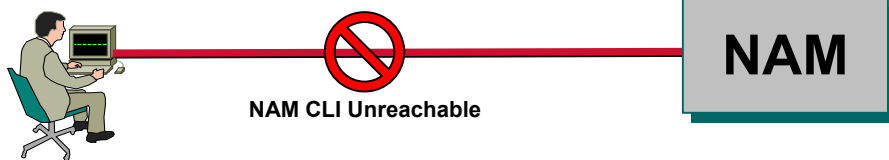


- Requirements
- Administration
- **Maintenance**
- Diagnostics & Troubleshooting Tips



NAM Maintenance

Resetting the NAM



NAM-1, NAM-2

- Native IOS - `device# hw-mod mod <NAM_mod> reset`
- CatOS - `reset <NAM_mod>`

NM-NAM

- `Router# service-module analysis-module slot/0 reset`



Resetting the NAM

Unfortunately, no network device is totally immune to the occasional lock-up. If needed, there are two ways to reset the NAM. If the NAM CLI is still reachable, simply enter the *reboot* command because this will reset the NAM. If the NAM CLI is unreachable, then simply reset the module from the CLI of the host.

NAM Maintenance

NAM-1, NAM-2 Image Upgrade



Application Image

hdd:1

1. Reset NAM using the maintenance image (cf:1)
2. Log in to NAM CLI with root
3. Retrieve image from FTP site and upgrade
4. Follow prompts
5. Exit NAM CLI
6. Reset NAM using the application image (hdd:1)

Maintenance Image

NAM-1/NAM-2 = cf:1

1. Reset NAM using the application image (hdd:1)
2. Log in to NAM CLI with root
3. Retrieve image from ftp site and upgrade
4. Follow prompts
5. Exit NAM CLI
6. Reset NAM using the application image (hdd:1)

Image Upgrade (NAM-1, NAM-2)

The NAM-1, NAM-2 cards utilize two images: a maintenance image and an application image. The maintenance image allows the NAM to be loaded with a basic operating system to perform maintenance tasks such as upgrading the application image. The application image contains both the NAM operating system and the NAM traffic analysis software. Either of these images can be updated by simply rebooting the NAM with the image you are not upgrading.

In other words, to update the application image:

1. Reset/reboot the NAM using the maintenance image.
2. When the proper image is loaded, connect to the NAM CLI and issue the **update** command with the *ftp URL* where the new image is stored as the command parameter.
3. Follow all prompts.
4. Exit the CLI.
5. Finally, reset the NAM to use the application image (default for a reset).

Note(s):

- To determine which image the NAM is using, you can use the *show module* command or session into the NAM. When using the application image, the *show module* output will indicate the software version being used by the NAM. If using the maintenance image, the software version number will not be the NAM release version and should be followed by an "m." If the NAM is booted using the maintenance image, the banner displayed when a session to the NAM is created will indicate that the maintenance image is being used.

NAM Maintenance

NM-NAM Image Upgrade



The NM-NAM contains three NAM software images:

- NAM application image on the hard drive - Source of the NAM Traffic Analyzer and NAM CLI
- Helper image in flash memory - Used to recover or upgrade NAM software images
- Bootloader image in flash memory - Used to specify whether to boot the NAM application image or the helper image

Upgrading Application, Bootloader, Helper Image

1. Log in to NM-NAM CLI with root
2. Reboot NM-NAM to Helper Image
3. Retrieve image from FTP site and upgrade
6. Reset NM-NAM

Image Upgrade (NM-NAM)

The NM-NAM cards utilize three images: the application image. A helper image used to manage the NM-NAM images, and a bootloader image used to boot the NM-NAM to the application image or helper image. Any of these images can be updated by simply rebooting the NM-NAM into the helper image and selecting the desired function.

Note: The bootloader or helper image are usually only upgraded on recommendation by technical support.

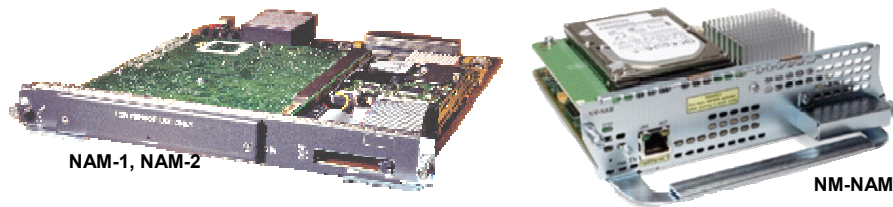
NAM Maintenance

Patch Installation

Patch Installation

From the NAM CLI

Root@localhost# patch ftp://user:password@host/full-path/filename



Patches - Incremental updates to software releases that are installed with the patch NAM CLI command. Patches are available only for the NAM application image

Patch Installation

To install an application image patch to correct any bugs or to provide additional capabilities simply use the patch command with the *ftp URL* of the patch location as the command parameter from the NAM CLI.

Note: Before patching NAM-1, NAM-2, make sure that the NAM-1, NAM-2 is currently booted using the application image.

NAM Maintenance Shutdown

NAM-1, NAM-2

Option 1 - Issue shutdown command from NAM CLI.

Option 2 - Issue module shutdown command from supervisor CLI.

Option 3 - If above two options fail, then press the shutdown button on NAM.

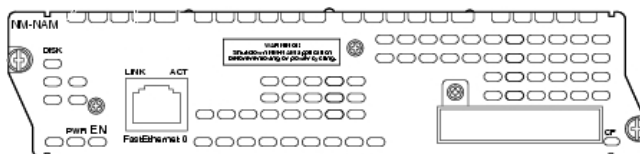
Status LED



NM-NAM

Issue shutdown command from Router CLI:

Router# service-module analysis-module s/ot/0 shutdown



Do not remove NAM until shutdown process is complete!

NAM-1, NAM-2: Status Light = Orange

NM-NAM: console message - %SERVICEMODULE-5-SHUTDOWN2:Service module NAM-Sensor1/0 shutdown complete

NAM-1, NAM-2 Shutdown

If it becomes necessary to remove the NAM from the host or to power off either the NAM or the host, the NAM must first be properly shut down to avoid damaging the hard disk.

NAM-1, NAM-2

There are three methods to shutdown the NAM-1, NAM-2. The preferred method is to issue the *shutdown* command from the root account of the NAM CLI. When the shutdown is complete, the status light on the NAM will be orange, and the *show module* output will indicate that the status of the NAM as down. The NAM also can be shutdown from the switch CLI. Note that the switch CLI can also be used to disable the NAM module. The difference is that the NAM cannot be reset until the module is enabled first.

If either of these methods fails, the NAM can be shutdown by pressing the shutdown button on the front panel of the NAM.

NM-NAM

The NM-NAM is shutdown from the router's Exec-level CLI by issuing the command **service-module analysis-module s/ot/0 shutdown**.

Note: The shutdown procedures can take several minutes.

CISCO SYSTEMS



- Requirements
- Administration
- Maintenance
- **Diagnostics & Troubleshooting Tips**



Diagnostics

Check System Alerts

CISCO SYSTEMS

NAM Traffic Analyzer

Help | Logout | About

Setup Monitor Reports Capture Alarms **Admin**

Users System **Diagnostics**

You Are Here: Admin > Diagnostics > System Alerts

Tech-Support System Alerts

Current system alerts: as of Mon 11 Sep 2006, 16:40:45 UTC

☒ Auto Refresh

	Date	Time	Message
1.	22 Aug	18:17:49	Completed capture hq-nam-82/Dtaport1_remotedisk
2.	13 Aug	22:30:10	Completed capture hq-nam-82/remote_capture_ALLSPAN
3.	26 Jul	14:17:31	%NAM-5-CONFIG_CHANGE: Configuration changed
4.	10 Jul	20:48:10	rmond connected to SUP (127.0.0.61)
5.	10 Jul	20:48:07	rmond 3.5(1) starting
6.	10 Jul	20:48:06	System time setting is sync with switch
7.	10 Jul	20:47:57	Module Online

[Clear](#)

View failures or problems that have occurred

NAM / Traffic Analyzer v3.5 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-32

Check System Alerts

You can view any failures or problems that the NAM Traffic Analyzer has detected during normal operations. This information can be viewed by going to the **Admin > Diagnostics > System Alerts** screen in the NAM Traffic Analyzer software.

As illustrated above, each alert includes a date, the time the alert occurred, and a message describing the alert. If you notice an alert condition and troubleshoot and attempt to solve the condition causing the alert, you might want to click **Clear** to remove the list of alerts to see if additional alerts occur.

Diagnostics

Check Audit Trail

Cisco Systems

NAM Traffic Analyzer

Setup Monitor Reports Capture Alarms **Admin**

Users System **Diagnostics**

You Are Here: Admin > Diagnostics > Audit Trail

Audit Trail

Current Data: as of Mon 11 Sep 2006, 16:45:39 UTC

Time	User	From	
08 Sep 2006, 07:48:26	admin	144.254.200.222	User login
08 Sep 2006, 07:44:22	admin	144.254.200.222	User logout
08 Sep 2006, 06:58:39	admin	144.254.200.222	Report created: Top Applications .
08 Sep 2006, 06:58:06	admin	144.254.200.222	User login
08 Sep 2006, 01:16:25	admin	171.69.223.105	SPAN deleted. Source(s):Fa3/1,Fa
08 Sep 2006, 01:16:00	admin	171.69.223.105	SPAN created. Monitor session:2
08 Sep 2006, 01:14:10	admin	171.69.223.105	User login
07 Sep 2006, 23:08:49	admin	10.21.89.164	User login

View activities that have occurred

Check Audit Trail

You can view a listing of recent critical activities that have been recorded in an internal **syslog** log file. Syslog messages can also be sent to an external log. The following user activities are logged in the audit trail:

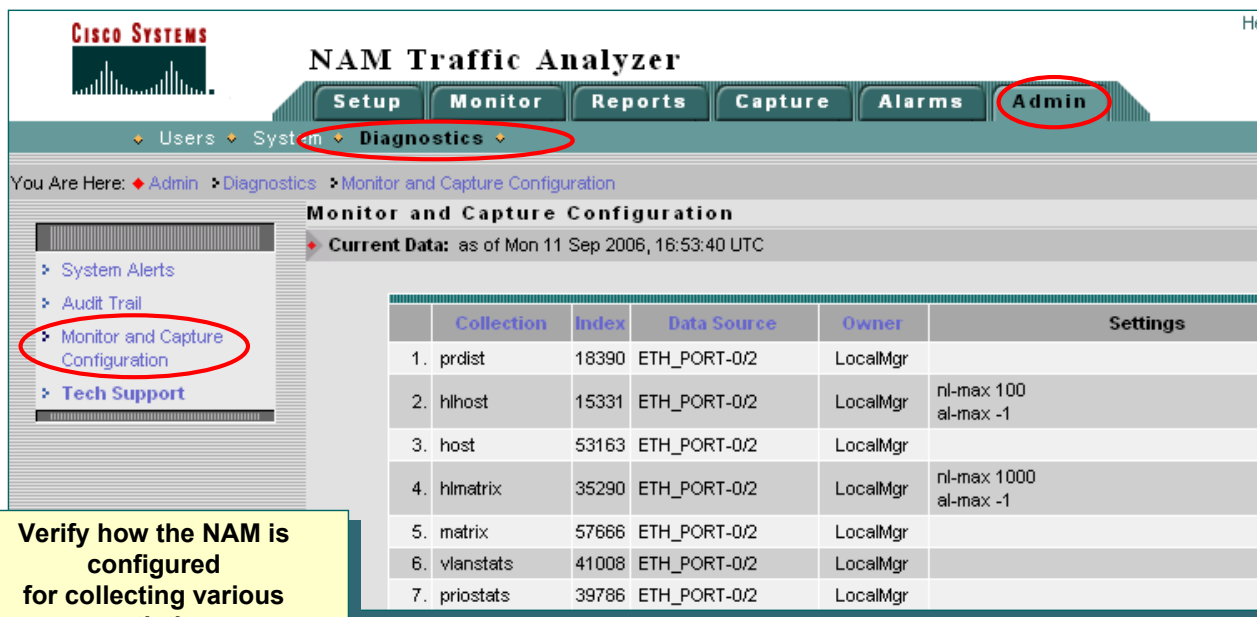
- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- SPAN changes
- NDE data source changes
- Enabling and disabling data collections
- Creating and deleting reports
- Starting and stopping captures
- Adding and deleting users

This information can be viewed by going to the **Admin > Diagnostics > Audit Trail** screen in the NAM Traffic Analyzer software.

As illustrated above, each activity includes a date, the user id, an IP address (in case of a remote access), and a note describing the activity. The internal log files are rotated after reaching certain size limit.

Diagnostics

Check Monitor & Capture Configuration



CISCO SYSTEMS

NAM Traffic Analyzer

Setup Monitor Reports Capture Alarms **Admin**

Users System **Diagnostics**

You Are Here: Admin > Diagnostics > Monitor and Capture Configuration

Monitor and Capture Configuration

Current Data: as of Mon 11 Sep 2006, 16:53:40 UTC

- System Alerts
- Audit Trail
- Monitor and Capture Configuration**
- Tech Support

	Collection	Index	Data Source	Owner	Settings
1.	prdist	18390	ETH_PORT-0/2	LocalMgr	
2.	hlhost	15331	ETH_PORT-0/2	LocalMgr	nl-max 100 al-max -1
3.	host	53163	ETH_PORT-0/2	LocalMgr	
4.	hlmatrix	35290	ETH_PORT-0/2	LocalMgr	nl-max 1000 al-max -1
5.	matrix	57666	ETH_PORT-0/2	LocalMgr	
6.	vlanstats	41008	ETH_PORT-0/2	LocalMgr	
7.	priostats	39786	ETH_PORT-0/2	LocalMgr	

Verify how the NAM is configured for collecting various statistics

Check Monitor & Capture Configuration

If reports and statistics are not being displayed as you thought they should, check how the NAM is configured for monitoring and capturing.

This information can be viewed by going to the **Admin > Diagnostics > Monitor and Capture Configuration** screen in the NAM Traffic Analyzer software.

If the name LocalMgr is displayed in the Owner column, the collection was configured by the NAM Traffic Analyzer.

Diagnostics

Check Messages Logged

CISCO SYSTEMS

NAM Traffic Analyzer

Setup Monitor Reports Capture Alarms **Admin**

Users System **Diagnostics**

You Are Here: Admin > Diagnostics > Tech Support

Tech-Support

Save This Page

Date

Fri Sep 8 18:12:31 UTC 2006

NAM settings

messages

```
Sep 5 18:34:20 nmtg-core2-6509-NAM httpd: PHP Warning: reset(): Passed variable is
Sep 5 18:34:20 nmtg-core2-6509-NAM httpd: PHP Warning: key(): Passed variable is no
Sep 5 18:34:20 nmtg-core2-6509-NAM httpd: PHP Notice: Undefined variable: span in
Sep 5 18:46:36 nmtg-core2-6509-NAM -- MARK --
Sep 5 19:06:37 nmtg-core2-6509-NAM -- MARK --
Sep 5 19:26:38 nmtg-core2-6509-NAM -- MARK --
Sep 5 19:46:39 nmtg-core2-6509-NAM -- MARK --
Sep 5 20:06:39 nmtg-core2-6509-NAM -- MARK --
```

Check further down for
messages with the words

- Error
- Failed
- Incorrect
- Warning

Check Messages Logged

The NAM also has a “tech-support” option that gathers diagnostic information from the NAM hardware and operating system. This information can be viewed by going to the **Admin > Diagnostics > Tech Support** screen in the NAM Traffic Analyzer software or by entering **show tech-support** from the NAM CLI. In either case, scroll down to the `/var/log/messages` information (toward the bottom) and look for key words indicating problems (error, failed, incorrect, warning). The information should indicate the source of the problem and provide you with a starting point for correcting it.

Finally, make sure that you review the release notes for any known issues and workarounds as well as the Installation and Configuration guide for additional Diagnostics.

Troubleshooting Tips

Verify Configuration

```
root@nmtg-core2-6509-NAM.localdomain# show ip
IP address: 192.168.137.82
Subnet mask: 255.255.255.252
IP Broadcast: 192.168.137.83
DNS Name: nmtg-core2-6509-NAM.localdomain
Default Gateway: 192.168.137.81
Nameserver(s): 171.70.168.183 171.68.22
HTTP server: Enabled
HTTP secure server: Disabled
HTTP port: 80
HTTP secure port: 443
TACACS+ configured: No
Telnet: Enabled
SSH: Disabled
root@nmtg-core2-6509-NAM.localdomain# show snmp
```

```
SNMP Agent: nmtg-core2-6509-NAM.localdomain 192.168.137.82
```

```
SNMPv1: Enabled
SNMPv2C: Enabled
SNMPv3: Disabled
```

```
community private write
community public read
community rootcse write
```

```
sysDescr Cisco Network Analysis Module (WS-SUC-NAM-2), Version 3.5(1)
Compiled 2006:06:12 14:51:24 by pwildi
Copyright (c) 1999-2006 by cisco Systems, Inc.
sysObjectID workgroup.1.3.1.1.2.291
sysContact Cisco Systems
sysName NAM
sysLocation RMON Lab
root@nmtg-core2-6509-NAM.localdomain#
```

NAM and Cisco Catalyst Switch must be in same subnet/VLAN.

Slow DNS may result in slow Web pages.

Web server enabled and client using correct port.

Third-party applications needs to use same community strings as set on the NAM.

Verify Configuration

You may lose connectivity to a device or other operational issues may arise because of a change in the operating parameters. Therefore, you should first verify that the operating parameters are correct. To do so, log in to the NAM, using the command line interface, and use the following commands:

- *show ip* (connectivity problems)
- *show snmp* (connectivity and data retrieval problems from a third-party application)

Troubleshooting Tips

Configuration Guide

Refer to the following Catalyst 6500 and 7600 Series Router NAM Configuration Note for additional information on the following topics:

- Netflow Data Export
- Error Messages
- Web Username and Password Guidelines
- Supported MIB Objects
- Local Interfaces in the NAM ifTable

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00805e351a.html

Troubleshooting Tips

The NAM also has a “tech-support” option that gathers diagnostic information from the NAM hardware and operating system. This information can be viewed by going to the **Admin > Diagnostics > Tech Support** screen in the NAM Traffic Analyzer software or by entering **show tech-support** from the NAM CLI. In either case, scroll down to the `/var/log/messages` information (toward the bottom) and look for key words indicating problems (error, failed, incorrect, warning). The information should indicate the source of the problem and provide you with a starting point for correcting it.

Finally, make sure that you review the release notes for any known issues and workarounds as well as the Installation and Configuration guide for additional troubleshooting tips.



Thank You!

We hope that you have found the NAM features to be an important part of your network-management toolkit.

Cisco Systems



NAM References

Chapter 5

- Cisco Network Analysis Modules (NAM)
NAM-1, NAM-2, and the NM-NAM
- Cisco NAM Traffic Analyzer Software v3.5



<Intentionally Left Blank>

Reference Materials

Many Cisco reference documents have been created to help users understand the use of Network Analysis Modules (for the Cisco Catalyst 6500 series and Cisco 7600 series NAM-1 and NAM-2 and the Cisco Branch Routers series NM-NAM) and its integrated Traffic Analyzer software. However, finding help and documentation can often be a challenge. This reference chapter has been created to assist you in your pursuit of additional product information. Below are links to documents and web pages that provide further details on these Network Analysis Modules (NAMs).

- **Cisco Catalyst 6500 and Cisco 7600 Series NAM (NAM-1, NAM-2)**
 - ♦ **Quick Start Guide ([URL](#))**
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html
 - ♦ **Product Literature (Data Sheets, Case Studies, Bulletins) ([URL](#))**
<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html>
 - ♦ **Troubleshooting Tips: Catalyst 6500 and 7600 Series Router NAM Configuration Note ([URL](#))**
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_installation_and_configuration_guides_list.html
- **Cisco Branch Routers Series NAM (NM-NAM)**
 - ♦ **Quick Start Guide ([URL](#))**
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html
 - ♦ **Product Literature (Data Sheets, Case Studies, Bulletins) ([URL](#))**
<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5644/index.html>
- **Cisco Network Analysis Module Software (Traffic Analyzer)**
 - ♦ **Release Notes ([URL](#))**
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html
 - ♦ **User Guide ([URL](#))**
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_user_guide_list.html

- **Other Related References**

- ◆ **Cisco Performance Visibility Manager ([URL](#))**

Cisco Performance Visibility Manager (PVM) is a new proactive network- and application-performance monitoring, reporting, and troubleshooting application for maximizing network availability.

<http://www.cisco.com/en/US/products/ps6768/index.html>

- ◆ **Differentiated Services – White Paper ([URL](#))**

Different applications have varying needs for delay, delay variation (jitter), bandwidth, packet loss, and availability. These parameters form the basis of QoS. This white paper describes how to use DiffServ for QoS Signaling.

http://www.cisco.com/en/US/tech/tk543/tk766/technologies_white_paper09186a00800a3e2f.shtml

- ◆ **NetFlow Services Solution Guide ([URL](#))**

This white paper is an overview of NetFlow benefits and includes technical overview of features, details about the NetFlow cache, export formats and NetFlow operation.

http://www.cisco.com/en/US/products/sw/netmgts/ps1964/products_implementation_design_guide09186a00800d6a11.html

- ◆ **Configuring SPAN, RSPAN, and ERSPAN - Catalyst 6500 Series ([URL](#))**

This chapter describes how to configure local Switched Port Analyzer (SPAN), remote SPAN (RSPAN), and Encapsulated RSPAN (ERSPAN) on the Catalyst 6500 series switches.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160a5a.html

- ◆ **Configuring VLAN ACLs – Catalyst 6500 Series ([URL](#))**

This chapter describes how to configure VLAN ACLs (VACLs) on Catalyst 6500 series switches.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160a7e.html

- ◆ **Configuring NetFlow Data Export – Catalyst 6500 Series ([URL](#))**

This chapter describes how to configure NetFlow statistics collection and NetFlow Data Export (NDE) on the Catalyst 6500 series switches.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160a2b.html

- ◆ **Performance Management Best Practices ([URL](#))**

This white paper details the most critical performance management issues, including critical success factors, key performance indicators, and a high-level process map for performance management. It also discusses the concepts of availability, response time, accuracy, utilization, and capacity planning, including a short discussion on the role of proactive fault analysis within performance management and the ideal network management system.

<http://www.cisco.com/warp/public/126/perfmgmt.htm>

- ◆ **Cisco Enterprise: QoS ([URL](#))**

Overview of Quality of Service with links to detailed white papers and other general discussions

<http://www.cisco.com/warp/customer/779/largeent/learn/technologies/qos/index.html>

- ◆ **Cisco IOS Quality of Service ([URL](#))**

Links to Quality of Service resources including white papers

http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html

- ◆ **Baseline Process Best Practices ([URL](#))**

Describes baselining concepts and procedures for highly available networks

http://www.cisco.com/warp/public/126/HAS_baseline.html

- ◆ **Quality of Service (Internetworking Technology Overview) ([URL](#))**

Detailed overview of QoS capabilities

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm

- **Online Bug Tracker**

Search for known problems on the Cisco bug tracking system tool, called Bug Toolkit.

To access Bug Toolkit, perform the following steps:

- Click on the link above (www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)
- Login to Cisco.com
- Click **Launch Bug Toolkit**.
- Enter the keyword **NAM** in the field to search a list of Cisco Software Products
- Then click **Next**.